2025

Strategy on the resilience of critical entities –

Standards for ensuring the proper operation of critical infrastructure - best practices and recommendations

RCB
Rządowe Centrum Bezpieczeństwa

1. How to use standards and best practices

1.1. What does it contain and for whom is it intended?

The document provides basic information on the organizational and technical aspects of critical infrastructure (CI) protection resulting from the provisions of Article 13 of the CER Directive[1] and the Standards on the Resilience of Critical Entities pursuant to Article 4 of the CER Directive (SotRoCE). It can serve as a set of specific guidelines for the construction, organization or operation of the CI protection system.

In the document, a reference can be found to the basic requirements and their impact on the process of threat identification and analysis and on the estimation of risks to which each CI operator is obliged. The document also describes the extent to which CI protection is correlated with tasks in the areas of business continuity[2] and cybersecurity, but also personal, physical, technical and legal security, as well as the objectives of the CI operator and its resources.

The document can be a source of reference for the creation of one or more security policies by CI operators, expert studies that are a source of knowledge for those who supervise CI, as well as for stakeholders, i.e. natural and legal persons, entities, public security and general security services that are involved directly or indirectly in the protection of CI.

The document is intended for CI operators, CI system coordinators and stakeholders performing CI tasks, as well as those interested in implementing selected aspects of CI security in their organizations.

The recommendations used in the appendix can be used to develop:

1/ documents of the coordinators of individual CI systems, which plan to include a set of provisions and strategies to be implemented,
2/ resilience plan, as referred to in Article 13 of the CER Directive,
3/ recommendations in the processes of design or construction of new facilities that could potentially be envisaged for the list of CI facilities.

[1] 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

[2] Business continuity is "the ability of an organization to anticipate and respond to incidents and disruptions in its operations in order to continue them at an acceptable level." Staniec, J. Zawiła – J. Niedźwiecki, ed., 2008. Zarządzanie ryzykiem operacyjnym [Operational risk management]. Warsaw: C. H. Beck p. 261.

1.2. What does it not contain?

The appendix is not a document containing a complete set of rules and information on critical infrastructure protection. It does not contain detailed technical instructions and organizational procedures; however, it can serve as an extensive checklist for verifying the CI operator's adopted requirements used in risk assessment processes or in processes related to raising CI security standards.

The description of some CI protection measures and rules to specific security areas is usually not obvious and unambiguous (there are measures that can be assigned in various areas), and cannot be considered definitive.

The authors of the study do not recommend a single method for risk assessment, as this is not possible in a diverse security environment.

1.3. Why conduct a risk assessment?

The principle of proportionality and risk-based activities is one of the key principles for the organization and functionality of the CI. It means that any measures taken to ensure the protection of CI should be proportionate to the level of risk of disruption to its operation. This applies both to the adopted model of CI protection, its types, as well as the forces and resources (assets) used. Considering the importance of this principle in the practice of the functionality of operators and coordinators of CI systems, it means taking measures to reduce the risk of disruption of CI, and indicating recommendations for prioritizing activities.

Before beginning any analysis related to risk (the impact of uncertainty on the objective(s) set), there are three important issues to keep in mind.

First of all, it should be remembered that risk estimation is a comprehensive concept, which, according to PN-ISO 31000, consists of the following processes:

1) threat identification,
2) risk analyses,
3) risk evaluation.

Second, the CER Directive in Article 4 draws attention to the essence of risk management and task-oriented collaboration resulting from the level of interdependencies with coordinators of other systems (cross-sectoral dependencies and interdependencies). For a CI operator, the management of CI risks and security is a recommendation for the proper management of the organization, where the public mission of the CI operator, understood as a set of duties and tasks to be carried out, may not always be the same as the business objectives, resulting from the participation of its

assets in the unified list of facilities, installations, equipment and services that make up CI.

Third, threat analysis and risk assessment and subsequent handling of risk is a cyclical process resulting from the regulations, standards, operational or quality regimes in effect for a particular CI, in addition to the CI operator's security policy or the recommendations of the CI system coordinator, if any have been adopted and implemented.

The best common denominator for conducting a coherent threat analysis and risk assessment is the theory of organizational business continuity management, or more specifically, its idea of the need for uninterrupted execution of an organization's critical processes.

A very thorough knowledge, understanding and description of the specifics of the organization's operations, both internally and externally, should be a priority activity, immediately preceding the risk estimation process. This means listing and systematizing the processes carried out in the organization. In practice, for this purpose, the most common recommendation is to conduct a so-called *business impact (event) analysis* (BIA – Business Impact Analysis), which results in the identification of critical processes.

In order to estimate risk to an organization in an effective and valuable way, the right conditions must be created for the entire process called risk management. The PN-ISO 31000 standard proposes the creation of a so-called management framework structure that provides the basis and arrangements to be implemented at each level of the organization. The BIA should be carried out for each process implemented by the organization, taking into account the dependencies and relationships between the various processes.

The results of the BIA should be:

- An assessment of the risk associated with the interruption of each process;
- An assessment of the financial and reputational losses associated with any process interruption;
- Estimation of factors that can lead to a reduction in the risk of failure in the initial stage;
- Estimation of the time required to remove the effects of the failure and restore business continuity;
- Identification of alternatives, factors with which business continuity can be maintained;
- Identification of alternative resources at the disposal of the organization;
- Determination of the cost of maintaining business continuity in terms of potential implementation of each alternative resource.

The basic assumptions and methods for conducting BIA and risk estimation are usually carried out in the following steps:

Step 1: identification of processes in the organization

A structured list of the organization's processes should be drawn up. Its creation begins by taking as a "starting point" the main objectives of the organization's operation. Their specific wording should be written in legal acts (e.g. statutes). The most relevant processes necessary for their implementation are then identified. These, in turn, should be further detailed by breaking them down into a series of sub-processes. Such a decomposition of objectives into processes is carried out until it is possible to present the main processes as a series of basic sub-processes (simple, unambiguous), for which it is possible to determine the specific resources necessary for their implementation.

1. The first main objective of my organization
    a. Main process 1
        i. Sub-process 1
            1. Resource 1
            2. Resource 2
        ii. Sub-process 2
            1. Resource 1
            2. Resource 3
    b. Main process 2
        i. Sub-process 3
            1. Resource 1
            2. Resource 4
        ii. Sub-process 4
            1. Resource 2
            2. Resource 4

Step 2: determination of effects – identification of critical processes

The BIA determines which *processes* are critical based on estimates of effect values at various intervals since their potential interruption. The method of proceeding boils down to defining a time scale that is uniform for the organization (e.g. 1h, 12h, 24h, 48h, 7 days, 14 days) and assigning to each *process* the value of the effects in subsequent time intervals. For instance, it is determined what financial and reputational losses the organization will incur if there is an interruption of the public mission, e.g. as a result of a power outage, which will last for 1 h, 12 h, 24 h, etc., consecutively. For the purpose of drawing up a consistent analysis, the catalog of effect types should be the same for the entire organization. Financial losses are indicated most often, but it is nevertheless worth considering reputational losses or legal liabilities as well. To facilitate the task of

identifying critical processes, a common qualitative scale can be developed and described for all types of effects. The selection of critical activities is done by analyzing data presented in tabular form, in which for each process the levels of all types of effects at different intervals are indicated.

	losses	1 h	3 h	6 h	12 h	24 h	3 days	7 days
sub-process 1	financial							
	reputational							
sub-process 2	financial							
	reputational							
sub-process 2	financial							
	reputational							
sub-process 3	financial							
	reputational							

Figure 1 Stages of SOC (security operations center) formation.

Step 3: identification of resources

The basis for estimating risk for an organization is to boil it down to risk to its broader resources. This is because it can be assumed that the risk of disruption or interruption of a process is the sum of the risk of unavailability (in the simplest terms) of all the resources necessary for its implementation. The next step, therefore, is to determine the minimum resources necessary to perform primarily the critical processes identified in step two. Identification of resources should also be done in a systematic way. For example, they can be identified and grouped as follows:

1) personnel resources (who is needed to carry out the activity and what competencies they should have),
2) material resources (what equipment, what materials are used to carry out the activity),
3) information resources (what do I need to know to perform the activity and with what tools),
4) financial resources (how many personnel and what resources are directly needed to implement the process).

Step 4: identification of threats and vulnerabilities

Adopting the principle of identifying specific resources makes it possible to determine the likelihood of various threats for them with much greater certainty. In this step, group work is particularly important, as it is difficult to predict the entire spectrum of dangers

on your own. Any suggestions for threats should be submitted for discussion. It is necessary to cooperate with a number of employees of the organization's units and to support each other with industry experts.

Both ISO/IEC 29147 and ISO 22301 consider vulnerability as a characteristic that enables a threat to affect the infrastructure. Vulnerabilities can be exploited by a threat that, by affecting the infrastructure, causes effects in the form of disruption to the organization. Vulnerability is not necessarily a factor that causes damage, but is a condition or set of conditions that can allow a threat to affect an organization, including the execution of key processes. Vulnerabilities can come from both internal and external sources and continue to exist until incidents or decisions within the organization itself reduce or remove them. Identifying them in the risk estimation stage is the easiest, and at the same time, in risk management, it is inevitable and also the most legitimate, since vulnerabilities suggest direct ways to deal with risk by preparing answers – what safeguards should be put in place in the processes of threat prevention, response and mitigation?

Step 5: risk analysis

Once the organization's list of critical processes is known and the possible losses from disrupting them are presented, a risk analysis should be performed. Typically, these are simple sums and/or products (e.g. probability x vulnerability x effect), but require determining the values of their components or factors. It is worth noting here that it has become accepted to define the probability of process interruption, while probability should be referred to the occurrence of threats to resources supporting critical processes. Special attention should be paid to those resources that have been identified in multiple processes.

Both risk and its factors can be measured quantitatively or qualitatively (e.g. descriptively). When possible and justified for ease of comparison, quantitative measures should be used. Probability and effects should be an area of quantitative and qualitative assessment, while vulnerability should be qualitative. In any case, it is useful to use scaling and selection of a risk matrix by the CI system coordinator and CI operator (assigning specific probability, vulnerability and effect values to scales, e.g., 1–5, 1–6, 1–7 or other scales tested and adopted in the security management process) using numerical ranges or a detailed description.

Step 6: risk evaluation

The final element of the risk estimation process is its evaluation. In everyday language, in the simplest terms, it means deciding whether to accept it or not. For each of the risks analyzed and quantified in step 5, taking into account the broad context of the organization, its objectives, its forces and resources, the views of stakeholders, etc., risks should be identified in all areas of security, including those related to CI, which require

further action no longer in the process of estimating but dealing with the risk (failure to accept the risk should mean drawing up a plan to reduce it). Methods of dealing with risk include, for example, transfer (sharing responsibility for risk, e.g. insurance), avoidance (e.g. by deciding not to continue risk-generating activities), reduction (introducing safeguards – leveling vulnerabilities), etc.

Added value for the organization can only be obtained if the risk analyses and assessments carried out are detailed and careful, and their authors are competent and experienced in this type of endeavor.

The organization's top leadership is expected to be involved in risk management and security management processes in its various areas by:

- determining the measures of risk and the characteristics needed to assess and control them,
- identifying risk hosts and a coordinator for risk management,
- ensuring the integration of the requirements in each security area with the supervisory competencies for those areas and the competencies of key personnel assigned to carry out the most important processes, services and dedicated tasks related to the public or (and) business mission,
- improving risk assessment activities and methods for strengthening resilience against threats and promoting a security culture,
- maintaining the ability to update risk management and response plans as part of their cyclical evaluation or as needed due to changes in the internal and external security environment,
- "leadership and commitment to leading and supporting personnel in contributing to the effectiveness of the BCMS[3] and its promotion of continuous improvement, and supporting other relevant leadership roles to emphasize their commitment included in their responsibilities".[4]

2. Recommendations and best practices for CI protection

It is important to remember that critical infrastructure protection cannot be understood as an isolated, independently functioning structure, and security aspects permeate all, even seemingly insignificant, spheres of the CI operator's activities.

[3] BCMS – Business Continuity Management System
[4] PN-ISO 22301:2020 Security and resilience – Business continuity management system – Requirements, pp. 25–26

Regardless of which types of protection are chosen and implemented by the CI operator, it should be borne in mind that four elements are crucial in the implementation of all their types:

(1) Conducting educational activities.
(2) Proper organizational structure of the security management division(s).
(3) Selection of the implementation strategy and its monitoring.
(4) Verification of the solutions adopted through tests, exercises, audits and inspections, and their update.

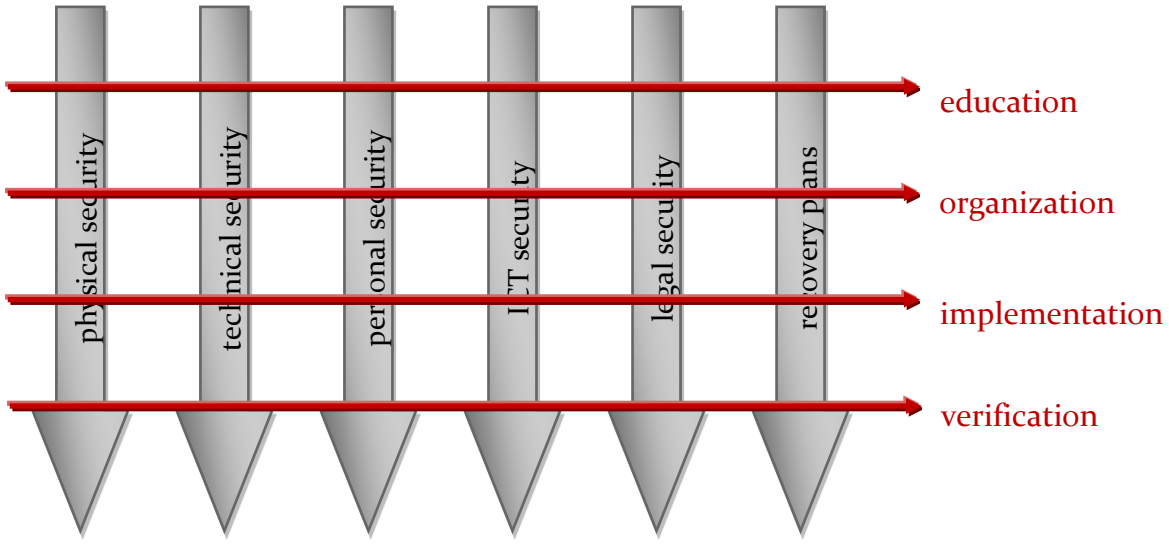


Figure 2 Cross-cutting activities for CI protection

2.1. Educational activities

Conducting education and awareness-raising activities is an essential, often underestimated and neglected, way to ensure CI security. These activities are aimed at bringing security rules closer to the general public and ensuring that employees have the right knowledge, understanding, application and attitude towards security rules.

Educational activities should be carried out in two stages:

- STAGE I – basic security training for newcomers.
- STAGE II – ongoing education and awareness activities for employees.

For the vast majority of an organization's personnel, security rules are unfamiliar, usually an impediment to daily work, and learning about them can be seen as boring and unnecessary. Therefore, it is very important to prepare an appropriate, practical and attractive awareness program.

The elements that can make up such a program are:

- basic training based on a scheme:
  - presentation of case studies,
  - imparting theoretical knowledge,
  - conducting exercises and workshops, and summarizing them in the form of agreed and implemented conclusions and recommendations,
- preparation and presentation of short educational films referring to basic security rules or current events depicting threats. Such videos can, for example, be presented on the organization's intranet,
- sending out information that constitutes threat alerts, such as about a virus spreading or a social engineering method being used by computer criminals,
- sending out an electronic periodical that reminds people of security rules in a short, attractive and clear form, especially with regard to current events. Another way to distribute the periodical is to present it in the form of a short video or an interactive website,
- visual awareness by hanging posters on security rules in the organization,
- competition (quiz) with prizes.

Three basic areas of education on the example of ensuring ICT security with the identification of sub-areas of particular relevance:

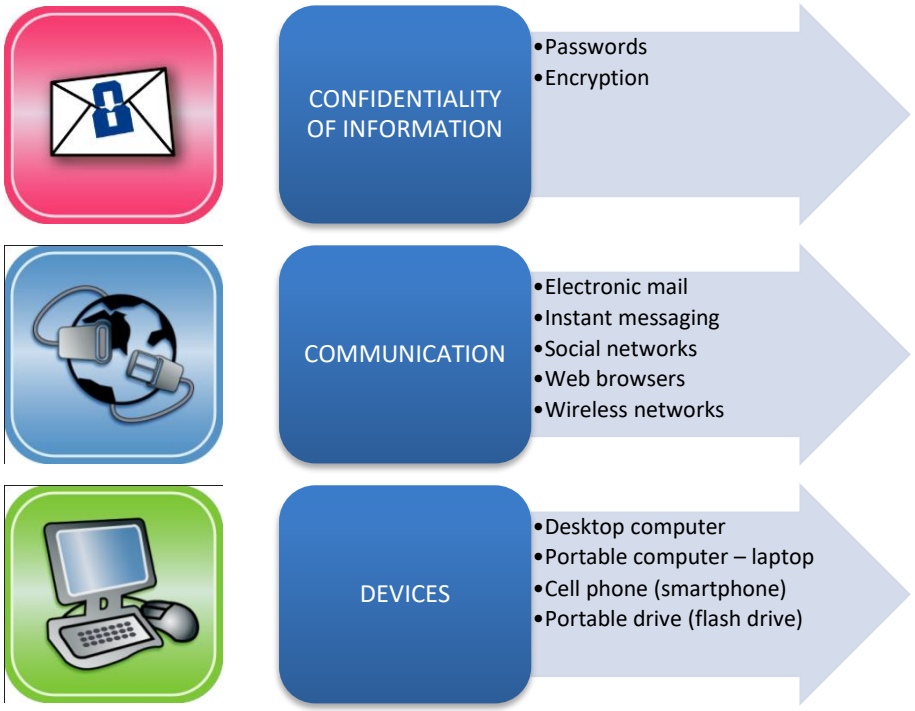


Figure 3 Basic areas of education in ensuring ICT security.

Educational activities should be extended not only to personnel whose responsibilities include CI protection tasks, but also to those not directly related to these tasks. All members of the organization should participate in CI protection – in response to adverse events, supportive activities are as important as the mainly executed ones.

Educational activities are an essential element in building an organization's security culture. Security culture means shared responsibility of the members of the organization for security, manifested by commitment and responsibility for processes regarding risk management, vulnerability to threat materialization, and management of response and asset recovery processes.

Without building adequate support from top management, it will be difficult to achieve the entrenchment of the security system and achieve improvements in the organization's resilience to situations of threat materialization, but also in terms of building adequate personnel readiness, implementing organizational, operational and technical changes, as well as investment and innovation. The essence of education and training activities for the management of the organization, is to build awareness of the importance of threat and risk factors and the ability to define tasks, authority and delegate responsibility for implementing, maintaining and improving risk prevention mechanisms at all levels of the CI operator's organizational structure. Top management, i.e. management board and management personnel, is expected to have a high level of awareness and competence in managing risk assessment processes and protecting and strengthening resilience for critical services in relation to security management in its various areas by ensuring that:

- security policy is established and up-to-date and consistent for all areas of security, and is consistent with the strategic direction of the organization and the respective CI sector in the country,
- individual security areas are integrated with the supervisory competencies for those areas and the competencies of key personnel dedicated to the most important processes, services or dedicated tasks in a given security area,
- mechanisms are in place for the continuous improvement of risk assessment activities and methods to strengthen the resilience of infrastructure and the protection of critical services, and to promote a security culture among all employees.

A key objective of educating the board and management, as well as risk owners or coordinators, should be to build the organization's capacity to ensure functionality and continuity of operations during emergencies. An important part of education is the importance of risk control, which is worth learning about, measuring and comparing in planning processes, as well as during tests, exercises and auditing processes, in relation to the requirements adopted by the CI operator.

In educational processes, it is worth encouraging management to participate in direct activities to promote the Resilience ~~Critical Infrastructure Protection~~ Plan and the organization's security management system on the principle that "the example comes from the top," and to attach importance to the importance of communication on this issue with the staff.

2.2. Organizational structure

Achieving and maintaining an adequate level of security involves creating an appropriate organizational structure, consisting of positions dedicated to working on CI security. In the structure of an organization, there may be a single unit responsible for its security (all types of security assurance) or security tasks may be assigned to different units according to their competencies, such as human resources (personnel security assurance), ICT (ICT security assurance) or infrastructure maintenance (technical security assurance).

Both models have their advantages and disadvantages.

One unit responsible for security	
advantages	**disadvantages**
• high possibility of coordination • single-person responsibility • integration of all aspects of security in a single organizational unit • independence	• less insight into the activities of other organizational units and the need to collect detailed information on all their activities • the need to include specialists in each type of security in the structure of the unit • limiting oneself to one's own task area

Table 1 Illustrative summary of advantages and disadvantages – in a single unit

Security tasks in various organizational units	
advantages	**disadvantages**
• high staff specialization	• dispersion of security information among many organizational units
• information on activities that may involve security is available inside the unit	• the need to coordinate the activities of many organizational units
• greater confidence in security personnel	• dispersion of responsibility, especially in areas of overlapping competence

Table 2 Illustrative summary of advantages and disadvantages – in various units

The choice of a particular model depends on the organization's adopted management style, requirements and organizational and financial capabilities.

Notwithstanding the above, the effectiveness of the chosen model requires close cooperation between all organizational units. The use of so-called "bridges", i.e. people who combine competencies or have knowledge and experience in the field of security and a selected part of the organization's activities can be helpful in this regard.

One method of deciding on the shape of the organizational structure is to adopt existing models of organizational structures, such as – in the area of ensuring information and communication security – the use of safeguards defined in PN-ISO/IEC 27002:2023-01 ~~17~~ Information security, cybersecurity and privacy protection – Information security controls.

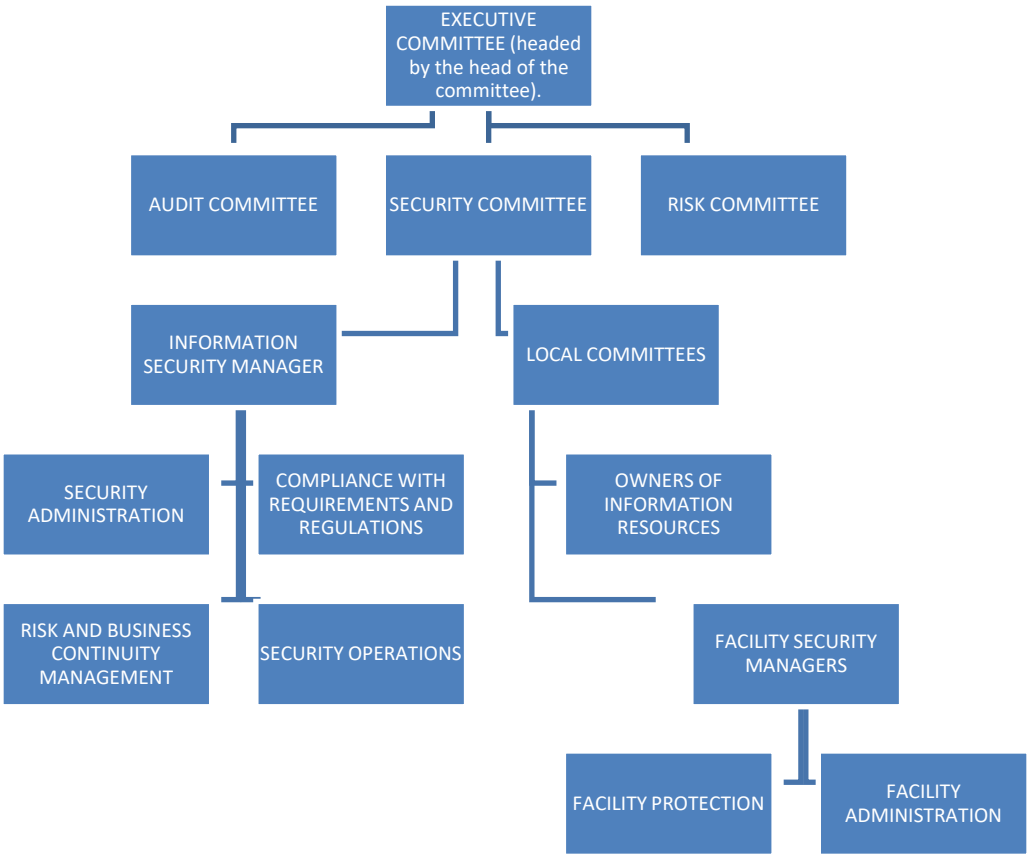


Figure 4 Illustrative organizational structure of the ICT security division

The above structure is recommended for the most expansive organizations which also have regional representations. It is recommended for those organizations that want to implement a complete Information Security Management System in accordance with ISO/IEC 27001. A simpler and more practical model is based on two categories of job positions (functions performed): mandatory and optional.

However, the best solution is a combination of both of the above systems. This is done by managing CI security in a centralized unit, and addressing activities related to the implementation of security, to the relevant organizational units.

Included in the group of mandatory positions are those that result from two important Acts related to information protection, namely the Act of August 5, 2010 on the Protection of Classified Information and the Act of May 10, 2018 on the Protection of Personal Data.

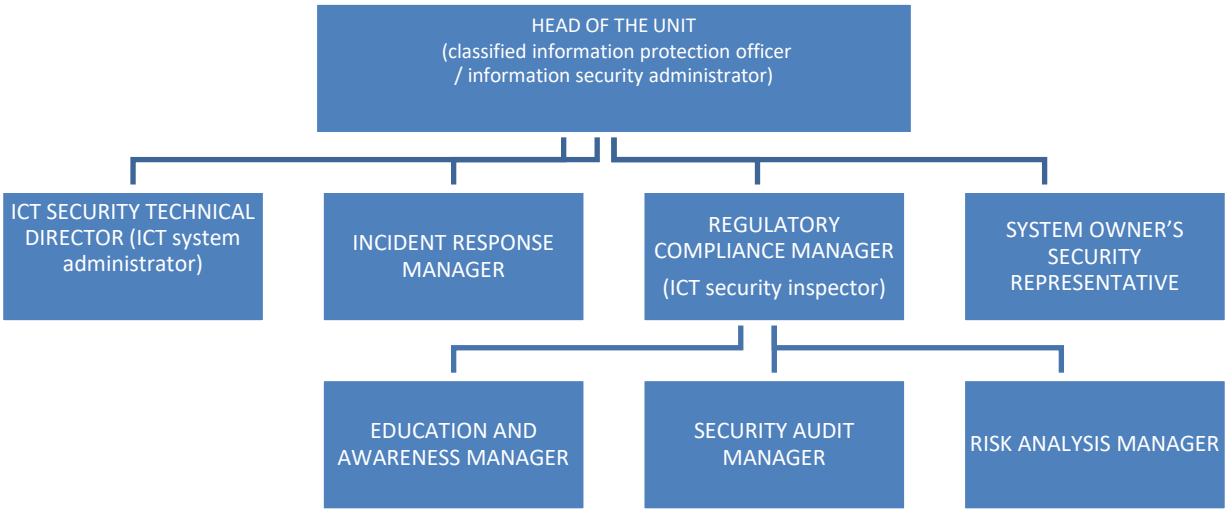


Figure 5 Organizational structure of the ICT security unit.

The following table contains a description of each position, with an indication of its mandatory or optional nature, an indication of which of the positions required by the aforementioned Acts the position corresponds to, and an indication of which of the other positions takes over the tasks of the function in question in the event of a decision to remove it from the organizational structure[5].

Table 3 Description of job positions under relevant Acts

JOB POSITION	POSITION REQUIRED BY ACT	TASKS	JOB POSITION TAKING OVER TASKS
SECURITY DIVISION MANAGER **(mandatory)**	Yes	Coordinate activities related to the overall provision of the required ICT security of the organization	N/A
IT SECURITY TECHNICAL DIRECTOR **(mandatory)**	Yes	Coordinate technical activities related to the overall provision of the ICT security of the organization	N/A
INCIDENT RESPONSE MANAGER	No	Coordinate the handling of reports related to violations of the organization ICT security	Regulatory Compliance Manager

5 For the detailed scope of the positions indicated in the Act on the Protection of Classified Information and the Act on the Protection of Personal Data, please refer to the contents of these Acts.

JOB POSITION	POSITION REQUIRED BY ACT	TASKS	JOB POSITION TAKING OVER TASKS
REGULATORY COMPLIANCE MANAGER **(mandatory)**	Yes	Supervise and control the proper design, implementation and maintenance of policies and mechanisms to ensure ICT security	N/A
SYSTEM OWNER'S SECURITY REPRESENTATIVE	No	Representation of the system owner, in order to control that security rules do not compromise the key functions of the proper operation of the system according to business demand	Regulatory Compliance Manager
EDUCATION AND AWARENESS MANAGER	No	Conduct continuous awareness and educational activities for all employee levels, with the main goal of raising awareness of the relevance of safety rules, the most important threats and how to respond in the case of their occurrence	Security Division Manager
SECURITY AUDIT MANAGER	No	Audit the compliance of the actual state with the accepted safety rules	Regulatory Compliance Manager
RISK ANALYSIS MANAGER	No	Conduct risk analysis for all existing and newly emerging threats	Regulatory Compliance Manager

Another example of a usable (adaptable) organizational structure is the one proposed in BS 25999 (replaced by ISO 22301:2020) for managing an organization business continuity.

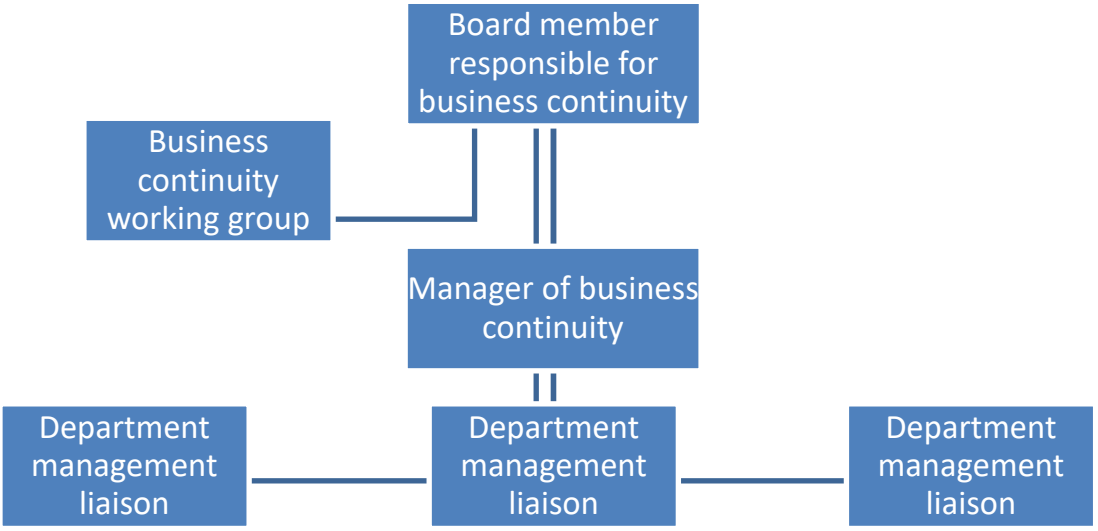


Figure 6 Illustrative business continuity organization structure

The business continuity working group should include management personnel from each organizational unit. The task of this group includes:

- control of resource allocation,

- establishing the organization business continuity priorities,
- establishing strategies for activities in line with the goals of the organization,
- spreading the importance of business continuity in the organization.

Department management liaisons are responsible for implementing business continuity processes in their subordinate task areas – this task is most often additionally assigned to managers at the operational level. Successful implementation of this model requires that all employees understand the purpose of their business continuity activities and their importance to the organization.

Whatever the model is adopted in the organization structures, the CI security unit(s) should be placed so that it is given an appropriate position, reflecting the importance of security principles to the organization. It is equally important to ensure that the security manager and their team are independent of other units in the organization. The interests of these organizational units are often in conflict, and inappropriately weighing security principles in favor of functionality and ease of achieving business and statutory goals can lead to serious disruption of the functioning of the organization. CI security activities should constitute a piece of the work and responsibility of every member of the organization.

2.3. Implementation standards

Implementing CI protection principles in an organization is not a short and easy process. Of course, much depends on the size of the organization, the previous level of security organization, and the preparation of personnel for such an implementation. Therefore, it is worth exploring the concept of the principles phased implementation, so that the entire process occurs systematically, in an orderly manner and faces as few obstacles as possible. The three most serious obstacles to implementing the protection principles are:

- employee resistance,
- maintenance costs,
- implementation costs.

The appropriate level of these obstacles makes the rules easier or more difficult to implement. If we assign measures to the level of difficulty and costs of implementation on a scale of 1–3 (1 – most resistance, highest costs, 3 – least resistance, lowest costs), then we can assume that we can calculate the ŁW (ease of implementation) indicator as a sum of these ratings:

$$ŁW = Op + Ki + Ku - 3$$

where:

Op – the value of the resistance level of employees,

Ki – the value of implementation costs,

Ku – the value of the maintenance costs.

We subtract the value of 3 as the value that the indicator always takes as a minimum. In this way, the indicator values are given clearer values on a scale of 0–6.

In addition, the proposed security rules have different levels of effectiveness, which can be called WE (efficiency indicator). We can also evaluate them on a scale corresponding to the ease of implementation indicator, that is, they will take values in the range of 0–6 (0 – least effective, 6 – most effective).

Based on the above valuation, we are able to create a graphical representation of indicator values for all proposed security principles and techniques. By dividing the area showing the level of effectiveness and ease of implementation into quadrants, we get the assignment of each security principle to four areas:

I – rules not very effective and difficult to implement,

II – effective rules, but difficult to implement,

III – rules not very effective, but easy to implement,

IV – rules that are effective and easy to implement.

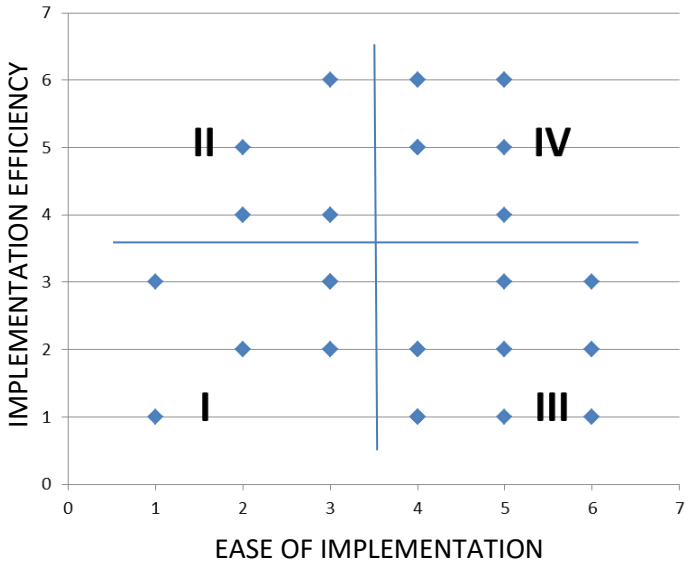


Figure 7 Four areas of security rules assignment.

Such a breakdown will allow us to identify the different phases, assign rules to them and develop an implementation, such as a three-stage one:

- Stage I – at this stage, high-efficiency rules easy to implement are being implemented.
- Stage II – at this stage, low-efficiency rules easy to implement and high-efficiency rules difficult to implement are being implemented.
- Stage III – at this stage, low-efficiency rules difficult to implement are being implemented.

Evaluating the rules used from the point of view of implementation difficulty is not an easy task. There are no accepted clear standards for such an assessment. It may depend on the individual characteristics of the environment in which the rules are implemented, and on the individuals responsible for it. Nonetheless, experience shows some universal features of these rules, which make it possible to evaluate them with a high degree of probability. The following shows what a sample evaluation table might look like with indicators of ease and effectiveness of implementation, and the final assignment of a given security rule to an implementation stage.

Table 4 Example of a table for evaluating implemented security rules

ELEMENTS OF THE SECURITY ASSURANCE SYSTEM	EASE OF IMPLEMENTATION INDICATOR	EFFICIENCY INDICATOR	IMPLEMENTATION STAGE
GENERAL			
Positions and scope of responsibility			
Education and awareness			
…			
PHYSICAL SAFETY			
Designation of safety zones			
Patrols inside the facility			
…			
TECHNICAL SECURITY			
Own water intake			
Power generators			
ICT SECURITY			
Software security			
Workstation protection			
PERSONAL SECURITY			
Visual identification of the employees the organization			
Controlling access to security zones			
BUSINESS CONTINUITY AND RECOVERY PLAN			
Testing the plan			

2.4. Verification of adopted solutions and their update

The measures taken by the organization to ensure CI security in the area should be reviewed. The following is verified:

- the adequacy of the adopted assumptions and plans in relation to the goals and priorities of CI protection,
- the correctness of the identification of key CI processes and the services that support them,
- the correctness of the assignment of roles and responsibilities,
- the effectiveness of the implemented solutions in relation to the level of risk of disruption to CI,
- the effectiveness of coordination and management of an adverse event,
- the usefulness of procedures and plans,
- the efficiency of the process of updating plans and implementing lessons from incidents into these plans.

Verification includes:

- exercises,
- audit processes,
- self-esteem,
- compliance management.

2.4.1. Exercises

Exercises are the only way, other than operating under real threats, to practically verify the measures taken to protect CI. They provide an opportunity to develop teamwork, improve competence, increase confidence in one's own abilities and level of knowledge. Exercises are also an opportunity to convince the organization staff of the desirability of emergency preparations – they show what problems could occur in the organization if the organization is not prepared for such problems.

Exercises should include in their scope all implemented types of CI protection (not necessarily at the same time), as well as the preparation of people who have been assigned roles and responsibilities as part of CI protection.

Maintaining the realism of exercises is one of the basic requirements for conducting them. However, it is important to keep in mind that it should not cause negative effects on CI and the organization, so it should be planned in such a way as to minimize the risk of actually disrupting CI as their result.

Every exercise should have clearly defined objectives and be carefully planned. After completing the exercise, make an analysis to check the achievement of the objectives. There should also be a report with recommendations for changes and a timetable for their implementation.

The scale and complexity of the exercise should be matched to the organization size and CI protection goals. The scale and complexity of an organization processes should also be taken into account when

determining the frequency of exercises – conducting a exercise once does not maintain organizational agility and does not take into account changes in the organization. Only regularly repeated exercises are a form of confirmation of the maintained effectiveness of the solutions adopted.

2.4.2.Audit processes

The tool used to assess the state of the CI protection system is an audit. It is one of the most important elements of this system. As a process of checking whether the measures taken are in line with the assumptions and whether the assumptions are effectively implemented, it is a material for obtaining information on the current level of protection, its status in relation to the functioning legal regulations and common security standards. One of the goals of the audit is to improve the level of security and increase the effectiveness of the solutions used by revealing resources not used or misused and potential gaps and vulnerabilities in the system.

A properly conducted audit should answer the following questions:

- Is the CI protection system functioning according to the adopted rules?
- Is there evidence (records) that the system is working?
- Is the system adequate for the threats and values protected?
- Is the CI protection system working properly and can it respond effectively to adverse events?
- How were the types of threats that may arise in connection with CI tasks and functions determined?
- What existing factors have a compounding and neutralizing effect on the threats, taking into account the people, places and time of their occurrence?
- What ways and countermeasures should be taken to neutralize threats and reduce the vulnerability of CI to these threats?

The following forms can be used in the auditing process:

- summary security audit – for the facility, the process and the entire organization,
- extended safety audit – referring to the facility and process carried out on the basis of the summary audit, when any of the evaluated parameters did not reach the desired level,
- full security audit – a comprehensive process that assesses the organization.

Audits should be conducted at set intervals and the results presented in the form of a report to the organization's management. Audit processes should be conducted objectively and independently, and competent people from within or outside the

organization can be used for this purpose. This good practice should also be applied to the self-assessment process.

In some situations, it is reasonable to use an external audit to verify the adopted solutions (lack of competence on the part of the organization, a legitimate need for an independent assessment, etc.). In such cases, it is important to keep in mind:

- service contract guaranteeing the confidentiality of the information collected by the auditors during their work,
- monitoring access to critical facilities verified by auditors (for example, when verifying a server room, auditors should be subject to the same restrictions as other people who are temporarily granted access to protected premises),
- establishing rules for access to key documents of the organization, i.e., what kind of audit notes can be taken, what documentation handed over during the audit can be taken outside the audit site (auditors' own work outside the audit site), rules for confirming the hand over and receipt of documents.

Those conducting the audit must have valid security clearances issued by authorized services, appropriate to the classification level of the documents being audited.

2.4.3. Compliance management

Compliance management is a set of processes designed to ensure that the state of assets (including CI assets) is in continuous compliance with the CI operator's security policies. Unlike projects and programs that inherently involve changes in the security environment, the task of compliance management is to maintain a state that ensures the expected level of security (preventing uncontrolled or harmful changes). Compliance management processes are linked to other asset management processes (asset management) and partly use the same solutions, e.g., shared databases.

In order to efficiently manage compliance, specialized IT tools are increasingly being used to monitor the compliance status of assets on-line, including assets that are specialized industrial control system solutions. These tools, in conjunction with other security solutions, provide management information that forms the basis for security improvement activities.

Security should not be an area that shapes competitive advantage. As a result, among the trends in the area of compliance management, it is becoming noticeable that communities of sector specialists are working together to try to develop security requirements that take into account the requirements of a particular sector to the best possible extent. The documents published by these communities are a valuable source of knowledge on security best practices.

2.5. Ensuring physical security

Ensuring physical security is a set of procedural, organizational and technical measures aimed at minimizing the risk of disrupting CI operations as a result of the actions of natural persons who have unauthorizedly attempted to enter or have entered CI. These consist of, among other things, direct physical protection and technical (electronic and mechanical) safeguards.
The direct physical protection and technical security implements its objectives through, among other things:

- Prevention
- Detection
- Transmission of information about the detection of an intruder (alarming)
- Delaying an intruder from reaching protected areas
- Responses/Intervention per incident

In addition to the aforementioned functions, the physical security system can perform

the functions of deterring an attacker, such as at the stage of prevention (e.g., information boards), alarming (external sirens) and intervention (calling for lawful behavior). The evidentiary function is also partially realized in the case of video surveillance systems.

It should be noted that no amount of physical security measures will ensure total security. Protective measures only increase the likelihood of effective counteraction.

The implementation of the physical security system should proceed in the following steps:

- determination of protected entities (elements),
- adopting basic design assumptions[6] for the system (determining who might be a potential attacker and their characteristics),
- assessment of necessary delay times for anticipated attack scenarios,
- establishing protected zones and rules of access to them,
- establishing technical support measures (technical security),
- development of procedures for the system operation (including people),
- installation and configuration of system components,
- system test,
- procedure overview,
- a test of the entire security system,
- systematic reviews of the system.

[6] In English-language literature they appear as *design basis threat (DBT)*.

Making assumptions about the knowledge, skills, equipment and determination of potential intruders is a key part of designing a physical security system. A good technique is to analyze who might be interested in unauthorized access to the protected resource. Here we mainly consider the attractiveness of the protected element to certain groups of intruders.

For example, entry to a protected heap may be of interest to a paratrooper or a thief of materials stored on the heap (e.g. fuel), and access to state security information classified "top secret" – to the intelligence of a foreign country.

Physical attacks on and incidents involving critical infrastructure are not at all uncommon. Here are some examples of breaches related to physical security breaches.

Table 5 Examples of attacks on critical infrastructure

Type of violation	Time/location	Description
Terrorist attack	April 19, 1995 Oklahoma City USA	Explosion of a truck filled with 2300 kg of ANFO[7] in front of the federal building in Oklahoma City. 168 people were killed and more than 680 injured. The attack was carried out by Timothy McVeigh, who was linked to right-wing extremists.
Terrorist attack	February 24, 2006 Abqaiq Saudi Arabia	An attempted attack on the world's largest oil refinery. The attackers tore through the outer fence, blowing up one of the accompanying cars. The bombers' other cars exploded after being fired upon by guards before crossing another fence. The attackers were well prepared, armed and equipped. News of the attack pushed up oil prices on the market.
Protest	July 03, 2007 Bełchatów Poland	Environmentalists broke into the power plant site, climbed the cooling tower and made a "Stop CO_2" slogan.
Protest	December 03, 2008 Konin Poland	Environmentalists broke into the power plant site, climbed up the chimney and launched a protest against greenhouse gas emissions.

7 ANFO (Ammonium Nitrate Fuel Oil) – an explosive obtained by soaking ammonium nitrate (NH_4NO_3) in liquid fuels.

Type of violation	Time/location	Description
Terrorist attack	July 21, 2010 Baksan, Kabardino-Balkaria Russia	Several perpetrators forced their way into the hydropower plant, killing two guards. Two of the three generators were blown up. The perpetrators were armed with machine guns and anti-tank grenade launchers.
Terrorist attack	January 16, 2013 In Amenas Algeria	Militia attack on gas field, resulting in four-day hostage situation. The death toll was 67. Production at normal levels resumed after 20 months.
Violation of airspace	January 03, 2015 Nogent-sur-Seine France	Drone entry into the nuclear power plant site.
Protest	March 18, 2015 Fessenheim France	An international group of environmentalists invaded the site of a nuclear power plant, demanding its closure.
Violation of airspace	March 19, 2021 Buquyaq Saudi Arabia	Attack by 6 drones on the Saudi Aramco refinery. Causing destruction, fear and unrest on the financial markets.
Cyber attack	April 29, 2021 USA	Ransomware attack on an important fuel pipeline. Colonial Pipeline Co. paid a ransom of $5 million.
Cyber attacks	Year 2022	Numerous ransomware attacks targeting CI (including power plants, water treatment plants, hospitals) and government entities, with the goal of restricting or disabling a particular service.

2.5.1. Organizational and preventive actions

Tasks in the area of ensuring physical security are carried out, among other things, by providing continuous 24-hour direct physical protection of CI facilities, equipment, installations and systems. Direct physical protection should be performed by an internal security service or entities operating in accordance with the Act of August 22, 1997 on the Protection of Persons and Property (Journal of Laws of 2021, item 1995). This will ensure, among other things, that those carrying out this protection can use, lawfully, direct coercive measures.

To ensure the effectiveness of the physical security system, it is a good practice to divide the site where the CI is located into

protection zones[8] and design them according to the principle of defense in depth (layers of protection). Sometimes the outside zone outside the facility is also determined.

Each zone must be designed to slow down the actions of a potential attacker as much as possible, and the intensity of security forces and measures should increase as potential attackers approach the zone protecting key elements of the organization infrastructure. As a result, this will deter the attacker or allow more time for a threat-appropriate response from the security system or qualified assistance.

An example of division into protection zones (from the most protected one):

1 – internal protection zone,
2 – contour protection zone,
3 – peripheral protection zone,
4 – perimeter protection zone,
5 – external surveillance zone.

Regardless of the functioning protection zones, or in the absence of separation of such zones, it is necessary to determine the conditions under which the level of protection is strengthened by applying additional (specified for a given degree of strengthening) protection measures, including, first of all, organizational and procedural ones.

The procedures concerning the following should be implemented:

(1) rules for entry of employees, trade partners, suppliers, contractors, subcontractors and visitors into protection zones and entry of their vehicles, and rules for movement within the facility, including: the process of registration, issuance of badges (passes/cards/PINs), assignment of the level of access privileges to individual zones, methods of authorization of access to individual protection zones and ongoing supervision of the place of stay, the possibility of control of authorization to stay in the zone, the possibility of personal searches, control of vehicles as well as items brought in or transported to the facility in the manner specified in the internal regulation of the entity, etc.;

[8] Protection zone – an area, together with the resources located therein, for which physical security requirements have been defined.

(2) rules for the use of identification elements (passes/keys/codes/PINs/cards), including: registration of identification elements, rules for storing and issuing keys to rooms and protected areas, periodic replacement of codes, procedure for issuing and granting cards;
(3) rules for granting and revoking access privileges, changing the level of access privileges, and issuing and revoking badges;
(4) inspection of security measures, including: those responsible for inspections, inspection intervals, inspection authorization documents, inspection protocols, etc.;
(5) servicing of technical measures to ensure physical security, including: periodic maintenance in accordance with technical documentation, contractually specified troubleshooting times, etc.;
(6) testing of security assurance measures, including the conduct of penetration tests and their course, those responsible for the tests, established testing time periods, etc.;
(7) ways of security response to certain types of events. Including strengthening individual protected sections in case of dysfunctional security assurance elements (e.g., failure of ACS, IAS, or VSS).

When building a facility that will require protection, it is important to remember the basic principles of security: deterring potential intruders, early detection of an attack, delaying the intruder (extending the time of attack) and efficient intervention. Consideration should be given to the use of urban, landscape, architectural and construction solutions that enhance security and ensure the strength and stability of structures, fencing, the possibility of security zoning and other solutions for the physical security system. It is advisable to conduct a risk analysis for the facility under construction in order to properly implement such solutions.

The conspicuous presence of physical security system measures (fences, nets and their capping, CCTV cameras, lighting, presence of security personnel) discourages potential aggressors. However, it should be borne in mind that not all security measures should be exposed, so as not to compromise the security of information about the construction of the facility security system. In addition, it is advisable to cover the documentation describing the physical security system used with adequate protection against unauthorized disclosure.

Regular, periodic inspections of the external condition of the surroundings of the protected facility (protection zone) should be carried out, taking into account access to the facility and the possibility of visual and technical observation, and the adjustment of the site, removal of

obscuring vegetation, trees, etc. inside and outside the facility should be carried out consistently, periodically and in accordance with the established pattern. Use of natural plant barriers should be considered (to slow down or even discourage potential intruders), such as roses or low-growing thorny shrubs such as barberries, which stand up well to pruning and can be easily shaped.

A command and coordination center for the physical security system in the organizational unit should be established and equipped with an integrated information system (VSS, IAS, and ACS) for any abnormal conditions occurring in protection zones. The integrated system will allow security personnel to make quick decisions and take actions to neutralize possible threats. For particularly important facilities, construction of a command and coordination center for the physical security system should be considered in such a way that disabling the operation of a single center does not deprive the organization of the ability to fulfill this important function. This can be achieved, for example, by preparing a backup center, including competent replacement personnel, capable of taking over the tasks of the primary command center, or designing the center in a distributed model, i.e. operating in parallel from at least two different buildings (preferably far apart). The backup center should have continuously updated data from all functioning security systems (VSS, IAS, ACS and others). Persons with the authority to control technical security (technical physical security measures) should authorize the performance of these actions by combining a minimum of 2 independent unique identifiers (e.g.: PIN-card, PIN-biometrics, etc.). If the persons are from outside the organization, the need should be considered to carry out such work jointly with or under the supervision of the organization employee. It is good practice to require employee and external service technician access codes for possible configuration changes. In addition, the changes in question must be recorded in the CI documentation (e.g., Service Book, Serviceman Book, or other documents recording technical security events; e.g., Electronic Security System Book – in accordance with the Regulation of the Ministry of Internal Affairs and Administration of September 7, 2010 on detailed rules and requirements to be met by the protection of monetary values stored and transported by businesses and other organizational units – Journal of Laws of 2016, item 793).

After each incident, an analysis of the incident should be conducted and, if necessary, the protective measures in place should be adjusted to prevent future security incidents.

2.5.2. Models of direct physical protection[9]

Direct physical protection should be adapted to the circumstances of the CI and the environment (social, municipal, business and other) and the specifics of the threats.

The standard solutions for direct physical protection are organized in the form of:

- checkpoints (e.g., guard, control, observation) operating in permanent mode – 24/7, temporary – at selected times of the day, and ad hoc – incidentally.
- patrols (on foot and in vehicles).

The overall physical security assurance system should be characterized by the following features:

(1) **Flexibility** – necessary in the situation of an event beyond the ordinary events resulting from the operation of CI and described in the standard operating procedures of the security service;

(2) **Mobility** – enhancing the efficiency of protective processes;

(3) **Complementarity** – the complementarity of the various elements of protection;

(4) **Completeness** – the weakest part of the system limits its protective capabilities;

(5) **Inviolability** – each of the system components must be protected by another, and its destruction, damage or restriction of its functionality must be immediately and unequivocally recognized, and the system itself diagnosed as infringed.

In the course of direct physical protection, duty personnel perform the following: foot patrols inside as well as outside the facility, vehicle patrols, passenger traffic inspections, parcel inspections and vehicle traffic inspections.

There are three basic models of direct physical protection, which can be divided in terms of the deployment and level of mobility of security units:

(1) static model,
(2) mobile model,
(3) mixed model.

9 Drafted on the basis of a presentation by Chief Constable Richard Thomson – Civil Nuclear Constabulary, London, May 18, 2011.

Static model:

- the purpose of this type of model is to prevent outsiders from occupying the site for a certain period of time,
- this is the preferred model in situations where the loss of the facility is unacceptable.

Main features:

- multilayer protection,
- multilayer detection system,
- permanent security checkpoints.

Advantages:

- design simplicity,
- security (it is not possible for a security member to be in the line of fire of another security member),
- simple command,
- ease of preparing the security service to operate under the described system.

Disadvantages:

- lack of movement of security means that it will not react quickly in the event of an unexpected situation,
- exposure to trap car attacks,
- depending on the topography, this system may require a large group of security personnel.

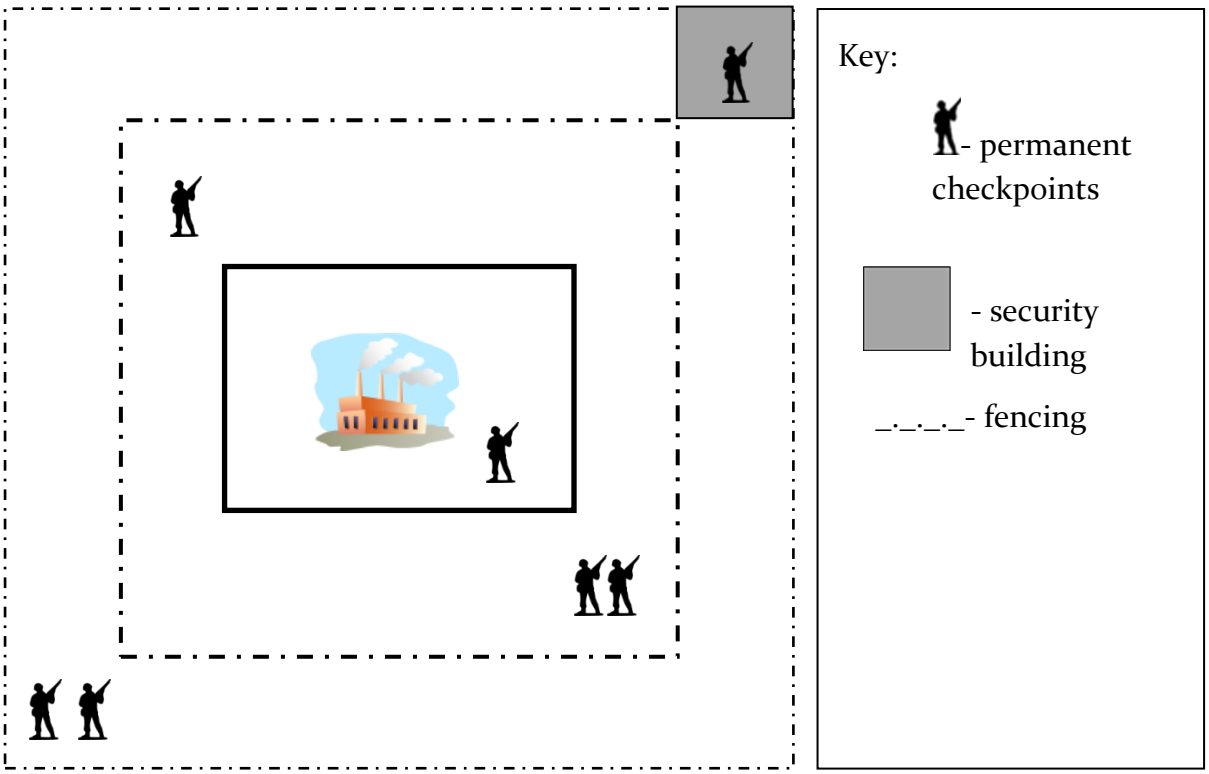


Figure 8 Illustration of how the static model works.

Mobile model:

- security services move freely around the facility and respond to emerging alarms or suspicious behavior.

Main features:

- various electronic systems are used to supplement the activities of security services,
- security service can move freely throughout the facility.

Advantages:

- flexible system – both patrols and security, adapt to given conditions or circumstances,
- size of the protective formation need not be large.

Disadvantages:

- the system does not work well for multi-point penetration attempts,
- the system requires a highly trained security formation that must constantly improve its skills through exercises and training.

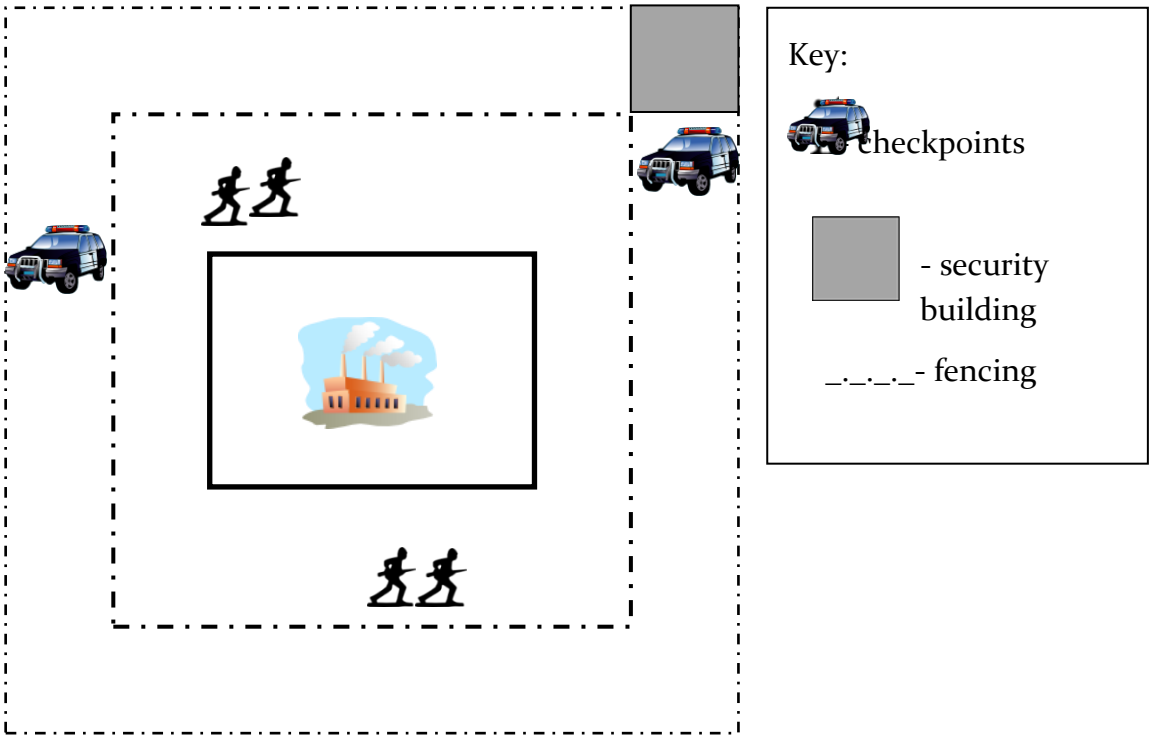


Figure 9 Illustration of how the mobile model works.

Mixed model:

- contains features of both models described above,
- works especially well for large facilities.

Main features:

- multilayer protection,
- static security elements coordinated with mobile patrols,
- permanent security checkpoints.

Advantages:

- patrols also present outside the facility site, which acts as a deterrent,
- mobile paroles provide a backup in the event of a penetration attempt,
- high efficiency,
- good situational awareness.

Disadvantages:

- requiring excellent training and equipment,
- complex system,
- costly.

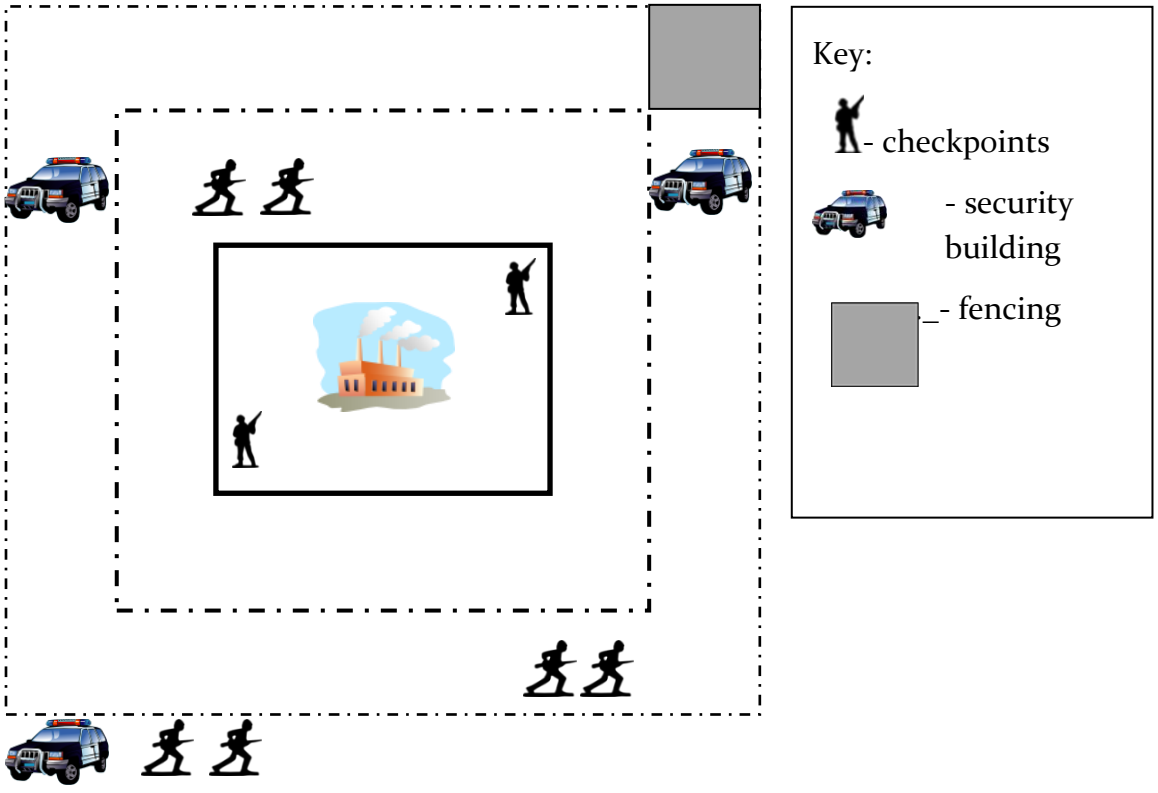


Figure 10 Illustration of how the mixed model works.

The choice of a specific security model depends on an assessment of the risk of disruption to CI, the technical and financial capabilities of the operator.

The scope of activities of security personnel should also include activities involving:

- protection of the CI site within its designated boundaries, from unauthorized access by all lawful and accepted security measures and undertakings,
- ensuring the safety of persons at the site or within the boundaries of the CI,
- preventing suspicious packages, such as those of unknown origin and those containing hazardous substances, from entering the CI site. For this purpose, x-ray machines, metal, radioactive substances and toxic substances detectors can be used, as well as forms of inspection of persons (search of clothes, luggage, body searches), inspection of vehicles (designated spaces of a vehicle: luggage, transport, tool, passenger spaces, chassis, etc.),
- protection of the CI property from theft, destruction or damage,
- preventing disturbances at the site and notifying the relevant superiors of events that cause a breach of order,
- receiving, storing, and releasing deposits (including weapons),
- constant surveillance of signals from electronic technical security systems,
- detecting threats of natural disasters, technical failures, and taking and coordinating actions to prevent and counteract their effects, until the arrival of the relevant services,
- notifying the relevant superiors of emergency events, security incidents, offenses, crimes.

Employees carrying out the protection of CI elements should be equipped with service weapons and ammunition and other means of direct coercion, as well as: personal bandages or medical kits, radio and telephone communications, flashlights, means of transportation and other equipment as necessary (e.g., helmets and bulletproof vests, gas masks). It is necessary to provide training in the skillful use of this equipment.

CI operators should ensure that security personnel have the opportunity to continuously upgrade and improve their skills regarding:

- an overview of security roles and responsibilities,
- conduct of security personnel in the field of fire safety. (e.g., active participation in evacuation),

- laws (tasks under the Act on the Protection of Persons and Property, rules of intervention, use of direct coercive measures and weapons, undertakings carried out as part of the various alert and CRP alert levels and other as necessary),
- first medical aid,
- intervention techniques and tactics,
- use of other means of direct coercion,
- techniques and tactics of using firearms,
- non-violent and forceful non-contact intervention techniques
- mine and explosive ordnance reconnaissance (basics).

It should be banned to bring weapons and ammunition, image recording devices such as cameras, camcorders, cell phones and tablets equipped with cameras, etc., into CI facilities by persons without special authorization or performing official tasks, which are regulated by internal regulations. For the duration of their stay at the facility, the above persons should deposit electronic devices that record video and audio in a depository room supervised by entities implementing physical protection of critical infrastructure.

2.5.3. Technical measures to ensure physical security[10]

Fencing, mechanical barriers, entrances and exits

If possible, critical infrastructure facilities should be completely fenced. Designated protection zones should also be fenced. The fence should meet the requirement of the longest possible defeat time for a potential intruder.

To this end:

- the design of the fence should make it difficult for people to climb over the fence, cut it, break it and knock it over,
- the height of the fence above the ground surface should make it as difficult as possible to climb over it,
- the lower edge of the fence should be permanently installed in the ground (e.g., embedded in concrete),
- should be equipped with a barrier to prevent undermining,
- should be equipped with barriers topped with barbed wire or razor wire fencing.

The fence can be built as:

- opaque with masonry construction or prefabricated concrete segments, etc.,
- transparent from mesh or panels,
- one or two sets with a safety corridor between them.

The fence should be able to operate with video surveillance systems, allowing observation of the outer fence and all entrances and exits of the protection zones, as well as intrusion alarm systems, allowing the earliest possible detection of an intruder.

Creating a buffer strip around the facility should be considered. If the location does not allow the creation of a buffer strip, mechanical barriers should be used to prevent intrusion, e.g. by a car. In this case, it is worth using elements like boulders or stones that have high resistance. Properly arranged, they can simultaneously create attractive surroundings of the facility.

Entrances to the CI site (if possible, it is a good idea to separate the entrances for employees from those for guests and visitors) and vehicle entry gates should be separated.

Entrances to the CI site for employees and passageways between protection zones should be equipped with passage activators (electric strikes, electric bolts), controlled by an Access Control System (ACS) that identifies a person and verifies their authorization using credentials, such as memorized information (PIN), or stored in an

[10] Sometimes the term "technical safeguards" is used.

ID badge (e.g., individual number or image of biometric features). In addition, the design of the entrance should allow visual identification of those entering by a security officer.

Whatever the proposal for the distribution of entrances, the objective should be to minimize their number. This facilitates access control and reduces the cost of

maintaining the physical security assurance system. However, if the number of entrances/exits is reduced, evacuation requirements should be kept in mind. Full registration in the ACS (at the entrance and exit) facilitates checking the completeness of evacuation (preferably in combination with attendance readers, located in collection areas for evacuation - the possibility of using the ACS function – Roll Call).

The height of vehicle entrance gates should be adequate for the fence, including capping barriers and protection against penetration beneath. Gate actuators (if the gate is not

manually controlled) should be equipped with appropriate measures to ensure full operation in all weather conditions. Gates should be equipped with barriers to prevent trespassing. As a rule, these barriers should be closed and opened only when the authorization of the person authorized to enter is confirmed by the access control system or a security officer.

There should also be a place for security personnel to inspect vehicles (cargo, identity of persons and authorization to be in the protected facility). Adequate equipment with

platforms, mirrors, cameras, tools and devices for verifying the authenticity of documents, etc. increases the efficiency of inspections. This place can be arranged in the form of a lock, bay, canopy, etc.It should also be ensured that there is inspection during loading and unloading of goods at the CI site (personal surveillance, using VSS cameras, etc.).

Lighting and illumination

If possible, critical infrastructure facilities should be fully illuminated to the extent that intruder detection, observation, identification and recording can be carried out effectively. When done properly, lighting also has a deterrent effect.

It is good practice to have a minimum of 100 meters visibility of the inner area of the facility under good weather conditions at night (no fog or precipitation).

Designated protection zones should be illuminated. The illumination should enhance the quality of observation realized with the video surveillance system. In selected areas, the illumination should support the detection of an intruder (protection zone and zones of access to the facility – so-called approach zones). Note that VSSs (in addition to those using thermal imaging cameras) use light reflected from elements of the supervised space. Some types of cameras can use not only illumination emitted in the visible band, but also emitted in the invisible band (near infrared). It is also important to remember to provide emergency power for the lighting of the space under surveillance, in case the power goes out.

Lighting is one of the least appreciated components of security systems and, as a rule, it should be capable of cooperating with video surveillance systems, BAS and the entire physical security assurance system. The appropriate use of lighting and illumination allows for the reduction of other security measures, due to the possibility of their better use.

Access Control Systems(ACS)

Access to protection zones as well as rooms or areas of key importance for CI operations should be controlled and restricted to authorized persons only. The ability to take such actions is provided by access control systems that:

(1) enable protection against unauthorized access to protection zones (including rooms);
(2) allow restricting the movement of unauthorized persons around the facility;
(3) allow the separation of protection zones, to which only authorized persons will have access;
(4) enable monitoring of the time of stay in the zone (including the room);
(5) facilitate the confirmation of employees' identities;
(6) ensure an appropriate level of access rights for contractors and visitors;
(7) facilitate the supervision of evacuation in situations when evacuation is required.

The ACS should be implemented in all protection zones and cover all entrances and exits for people and vehicle entry gates (or at least the used ones). Selected rooms inside the protection zones should be equipped with passage blocking devices controlled by an access control system or other method for identifying people entering the facility and controlling their access rights (key, video intercom). The ACS should be supported by a Video Surveillance System (VSS), only those employees who are necessary to ensure the

proper functioning of the zone or the equipment in it should be allowed to access individual zones.

The ACS can be programmed to prevent multiple granting of the access right in one direction. This is the so-called "anti-passback". Such a solution effectively enforces the need to register entry and exit from the protection zone and prevents allowing unauthorized persons to pass through protection zones if they have no grounds to do so. The presence of a user in a specific area to allow them to enter another area should be determined with the use of an access control system with the so called area controlled anti-passback.

While ensuring the control of entrances and people entering the facility, the control of exits and people exiting the facility should not be neglected. This is enabled by, among other things, monitoring the evacuation, such as in the event of a fire. When the ACS is shut down (e.g., passageways unlocked for evacuation purposes), in some cases of evacuation, it is necessary to introduce procedures for verification of its completeness, such as in the form of a person acting as a floor security duty officer or through the use of attendance readers, located in muster areas (the so called "Roll Call").

Video Surveillance Systems (VSS)[11].

A Video Surveillance System (VSS) is a system of cameras used to transmit the image (less often in combination with audio) from specific zones, areas or rooms in a closed receiving system aimed at supervising and enhancing the security of the zones, areas or rooms where the cameras have been installed.

A Video Surveillance System proves the most effective when selected zones, areas or rooms require constant control and supervision. The use of the VSS allows to:

- take protective actions from remote locations;
- identify the type of event;
- detect and identify persons and vehicles;
- detect any motion;
- analyze the background (e.g., a change in the arrangement of vehicle parking, package, suitcase, pallet displacement, etc.);
- record video and audio.

A typical VSS usually consists of the following components:

- fixed or moving cameras (with a tracking option);
- the so-called stage lighting system;
- infrastructure for video (and possibly audio) transmission and camera control;

[11] Video Surveillance System. In the past, the following terms were also used: "closed-circuit television", "utility television", and "surveillance television". This should not be confused with video monitoring systems for urban areas.

- video (recorders);
- a set of monitors and control devices located in a surveillance center (also called a monitoring center)[12].

The system fixed cameras should be installed on the boundaries of the protection zones with the entrances/exits and vehicle entry/exit gates, as well as the other entrances/exits and vehicle entry/exit gates used. The VSS installed at entrances to, exits from the protection zones should allow subsequent identification of persons, vehicles entering and leaving the above zones. Moving cameras should cover important on-site areas and roads. When planning the arrangement of cameras, it is important to avoid the so-called "blind spots", i.e. places, parts of areas or critical infrastructure facilities that could not be viewed using the VSS system.
Guaranteed lighting should interact with the VSS, covering entrances/exits and vehicle entry/exit gates, protection zone boundaries and other areas monitored by the system.

Intrusion and Hold-Up Alarm Systems

The Intrusion and Hold-Up Alarm Systems (IAS) are used to detect and record attempts of illegal (unauthorized) entry into protection zones, selected areas and rooms, and to provide, with the use of alarm buttons, information about the occurrence of an immediate threat.

The Intrusion and Hold-Up Alarm Systems are based on devices, such as among others device used to:

- detect motion in the zone covered by their operation;
- detect the opening of doors;
- detect the filling of building openings (entrances, windows, other openings);
- detect any damage to glass surfaces;
- detect any interference with the fence;
- warn of threats (emergency buttons).

A potential intruder should be detected as early as possible, so the IAS should cover the fencing borderline (perimeter protection zone), as well as entrances/exits and vehicle entry/exit gates (for each element separately) and selected rooms and buildings inside the protection zones.

Main roads and areas around entrances and exits can be equipped with alarm buttons installed in a visible place. Selected rooms or parts of

[12] The surveillance (monitoring) center should integrate all systems supporting the physical security assurance system (ACS, IAS, VSS).

protection zones can be equipped with concealed emergency signaling alarm buttons. The archiving of events should depend on the nature of the facility and it should include:

– **VSS system**
  - not less than 14 days of record, in facilities subject to the Regulation of the Minister of Internal Affairs and Administration of September 7, 2010 *on detailed principles and requirements to be met by the protection of monetary values stored and transported by businesses and other organizational units* (Journal of Laws of 2016, item 793);
  - not less than 30 days of record, in facilities subject to the regulation of the Council of Minister of May 29, 2012 *on physical security measures used to secure classified information* (Journal of Laws of 2012, item 683);
  - not less than 3 months of record, in facilities subject to Defense Standards. For CI facilities, it is suggested to keep the record for at least 30 days.

– **Access Control Systems:**
  - not less than 30 days of record, in facilities subject to the regulation of the Minister of Internal Affairs and Administration of September 7, 2010.

According to the regulation of the Minister of Internal Affairs and Administration of September 7, 2010 "in case of detection or reasonable suspicion of a criminal act, the related record should be archived in a way that does not reduce its quality. This also applies to the contents of the events memory of the BAS and ACS center, in case there is a connection between the contents of the memory of these devices and the criminal act. The contents of the memory should be secured, and then officially read and archived. The archival material should be assigned an archival category of documentation for the protection of the workplace (property), in accordance with the rules for handling archival materials." This means assigning the appropriate non-archival category, e.g., B2, in accordance with the applicable office and archiving regulations in this regard.

It is also important to keep in mind the emergency power supply required for electronic security systems, in case of mains power outage. For minimum standby times for backup power supply, see the relevant standards. For CI facilities, it is suggested to achieve standby times of:

–for the IAS – 60 hours,
–for the ACS – 4 hours,
–for the VSS with lighting – 4 hours.

It is important to remember that technical protection systems are designed, installed, maintained and operated to the highest quality standards. Persons performing services in this area should have a certificate of completion of a technical security officer course issued by a specialized continuing education institution operating in the educational system or have a valid certificate of entry in the list of qualified technical security officers.

It is important that the competence and qualification requirements of persons performing services in the field of technical security systems arise directly or indirectly

from laws, standards, technical specifications and industry standards, in particular with reference to the Law on the Protection of Persons and Property, military normative documents, PN-EN 16763 Services for fire safety systems and security systems, as well as the technical specification PKN-CLC/TS 50131-7 Alarm Systems, Intrusion and Hold-Up Alarm Systems, Part 7: Application Guidelines.

Examples of groups of standards to consider include:

- Alarm systems – Intrusion and Hold-Up Alarm Systems – PN-EN 50131,
- Alarm and electronic security systems – Electronic access control systems — PN-EN 60839-11,
- CCTV video surveillance systems for use in security applications – PN-EN 62676,
- Pedestrian doorsets, windows, curtain walling, grilles and shutters – Burglar resistance –PN-EN 1627:2021-11.

2.5.4. *Safety standards for CI operators in preventing, responding to and mitigating the effects of threats posed by incidents involving unmanned systems*

For many CI operators, unmanned systems provide a tool for threat monitoring, perform maintenance works and decision support to effectively improve the areas of physical, technical and ICT security in terms of ensuring the continuity of operation of processes resulting from the implementation of public or business missions and in terms of supervised tasks by control, security and counter-threat services. Unmanned systems can also be a tool of threat, the materialized result of which can be disruption, interruption or destruction of the CI functionality. To properly protect the CI, standards have been proposed to CI operators that recommend the basic requirements that a CI operator should meet in order to organize and improve the system for preventing threats, responding to threats and mitigating the effects of threats resulting from incidents involving unmanned systems. The system is part of the physical security threat analysis process, but it is also functionally integrated with the CI operator's existing risk and security assessment systems and resilience plan.

The application of the Standards affects the process of identification and analysis of threats and risk estimation for the CI prepared periodically or as needed by the CI operator. Conclusions from the CI safety assessments that take into account the effects of threats from incidents involving unmanned systems can influence outcomes and recommendations for public safety. The standards can form the basis for updating the rules of cooperation between the CI operator and the public services and public administration bodies overseeing individual CI systems.

2.5.4.1 Purpose of the Standards

The purpose of the Standards is to implement mechanisms to improve the resilience to threats posed by incidents involving unmanned systems and to improve the continuity of operations of key services and processes, as well as the functionality of key facilities, systems and equipment that make up the CI.

The use of the Standards allows the CI operator to indicate the priorities associated with exceeding the level of risk of effects for the CI accepted by the entity, adopted for representative threat materialization scenarios caused by incidents involving unmanned systems.

The application of the Standards allows the CI operator to organize a system for preventing, responding to and mitigating the effects of threats from incidents involving unmanned systems, as long as these threats are based on a risk assessment. The implementation of the Standards also supports mechanisms for improving security systems managed by services and entities carrying out tasks in the areas of public order and social, energy and transportation security.

2.5.4.2 Glossary of terms used

The definitions and terms used in the Standards shall have the following meaning:

a) **unmanned systems** – Unmanned Aerial Vehicle Systems (UAVS), Unmanned Ground Vehicle Systems (UGVS), Unmanned Surface Vehicle Systems (USVS) or Uncrewed Spacecraft Systems (USCS), prepared in a configuration that enables execution of specific missions and tasks along with control infrastructure and its operating personnel, consisting of the following components:

- **unmanned platform(s)** operating in air, water, land and space environments (*Unmanned Aerial/Flying Vehicle – **UAV/UFV**, Unmanned Surface Vehicle – **USV**, Unmanned Underwater Vehicle – **UUV**, Unmanned Ground Vehicle – **UGV**, Uncrewed Spacecraft – **USC***);
- **Ground Control Station/Panel – GCS/GCP;**
- **Ground Data Terminal – GDT**;
- **Communications and Data Transmission System;**

b) **drone, unmanned aerial vehicle** – common name for an unmanned aerial, water, ground or space vehicle;

c) **anti-drone systems** – systems designed to detect, recognize, identify and kinetically or non-kinetically neutralize elements of unmanned systems;

d) **unmanned intrusion** – unauthorized, intentional or unintentional, intrusion (by air, ground or water) by the unmanned system or its components into a specific area or zone affecting the CI components;

e) **unmanned aerial vehicle system or unmanned system operator** – any legal or natural person operating or intending to operate at least on unmanned aerial vehicle system or unmanned system;

f) **pilot of an unmanned aircraft** – a person responsible for the safe execution of the flight by the UAV either by manually controlling the flight or – if the UAV flies automatically – -by monitoring its course and maintaining the ability to intervene and change course at any time; a person who must have the requisite knowledge and skills necessary to ensure safe operation and proportionally to the risks associated with the type of operation in question; this person should demonstrate adequate health, if necessary to mitigate the risks associated with the operation in question, since the pilot is responsible for damage caused by the UAV they are piloting;

g) **unmanned system detection** – the ability to distinguish an unmanned system from the background of the surrounding space, leading to the detection, localization, and identification of the unmanned system (e.g., detection of an unmanned flying platform in the sky);

h) **recognition of an unmanned system** – the ability to distinguish an unmanned system from other types of objects in the airspace, on the ground or in the aquatic environment; as a result of the recognition process, it can be concluded that an

unmanned system has been recognized (e.g., distinguishing an unmanned flying platform from birds);

i) **identification of an unmanned system** – the ability to distinguish the characteristics of the unmanned system recognized, as a result of the identification process it is possible to identify main technical features, such as the structure or determine a specific model of the unmanned system of obtain the characteristics of the electromagnetic signal from the unmanned system control link and sensory data transmission from the unmanned system, and it is also possible to determine the location of the unmanned system operator's control station (e.g. determine the brand of the unmanned platform, indicate the pilot location as well as the platform location and trajectory);

j) **detection, recognition and identification of the unmanned system** – the on-going process performed either automatically (without the involvement of the anti-drone system operator) or semi-automatically (with the involvement of the anti-drone system operator); for the purpose of executing the process of detection, recognition and identification different reconnaissance devices are used, such as sensors, microphones and cameras; single or several technologies may be used in the anti-drone system at the same time, for examples sensors for radar, electronic and image recognition in various configurations and quantities, depending on the type of the anti-drone system as well as the CI characteristics and typology;

k) **unmanned system incapacitating** – the ability to neutralize, i.e. destroy, damage or interfere with the operation of the unmanned system or any of its subsystems or to make the operator unable to control the unmanned system to prevent further execution of the missions or tasks by the unmanned system;

l) **incident** – shall be understood as the situation referred to in section 5.9 of the Regulation of the Minister of Internal Affairs and Administration of July 22, 2016 on the catalog of terrorist incidents (Journal of Laws of 2017 item 1517);

m) **event** – shall be understood as a situation that has arisen as a result of an intentional or accidental action involving an unmanned system, which poses a threat to critical infrastructure and may cause negative consequences to public safety;

n) **mandatory protection area** – an area subject to mandatory protection resulting from the provisions of law or indicated by ministers, managers of central or provincial offices, properly separated and marked;

o) **zone of impact** – a zone that includes the area of mandatory protection along with the area beyond protection from which the impact from the unmanned system on the CI may occur.

2.5.4.3. The scope of application of the Standards

The Standards address threats that originate from intentional (deliberate) or unintentional human action, using an unmanned system operating in the air, water or on the ground.

The Standards will enable the CI operators to:

1. identify safety areas and assets vulnerable to threats posed by unmanned systems;
2. implement rules to analyze the threats and effects or likely effects of incidents involving unmanned systems;
3. improve risk management methodologies to prioritize specific actions related to protection against the effects of the use of unmanned systems;
4. identify mechanisms for analyzing opportunities and threats arising from changes on the market for manufacturers and users of unmanned systems and anti-drone systems;
5. monitor legal requirements and changes in the national security environment relevant to unmanned systems;
6. create opportunities for testing, organizing exercises and responding to incidents related to unmanned systems by employees and organizational units of the CI operator;
7. improve the rules for reporting and carrying out the missions of unmanned systems, when allowing foreign systems to operate in the CI area and use their own unmanned systems;
8. improve organizational and technical solutions for detection and neutralization of unmanned systems, if adopted and implemented as part of the security strategy;
9. create and improve methodologies for safe implementation of technical elements of protection against undesirable impacts of unmanned systems, in particular, in the field of:
    - 9.1. methods for assessing the effectiveness of technical solutions made by recognized third-party organizations, on the basis of functioning legislation and harmonized standards;
    - 9.2. multi-factor analysis of the CI operator's operating context that identifies constraints to the implementation of protection;
    - 9.3. determine the minimum requirements for technical elements of protection, if there are indications for the application of anti-terrorism standards.

The Standards support the decision-making process of government bodies in the field of:

1. vulnerability diagnosis of specific security areas, taking into account the threats posed by the use of unmanned systems;

2. implementation of conclusions to enhance the resilience of critical actors in each CI sector;
3. development of strategies to enhance supervised security, taking into account the use of unmanned and anti-drone systems.

2.5.4.4. Normative references

Regulations and requirements for unmanned systems derive directly or indirectly from the European and national legal system, having sources in the regulations of the European Parliament and the Council of the European Union and in the following laws: aviation law, telecommunications law, law on protection of persons and property, on anti-terrorist activities, crisis management, as well as the implementing regulations for these laws.

The requirements that define the organizational, technical, competence standard, as well as the training and professional development system, are also covered by industry and sector requirements, guidelines and rules or declared standards.

Requirements may also be derived from the CI operator's security policy and the documents of individual CI system coordinators.

2.5.4.5. The scope of preparatory work of the CI operator to decide on the development of a system to prevent, respond to or mitigate the effects of threats posed by incidents involving unmanned systems

2.5.4.5.1. Defining the context of operations of the CI operator

The operator defines external and internal risk factors that may affect their operations. The identification of these factors, along with the requirements included in the SotRoCE, forms the basis for launching the process of threat analysis and risk assessment and developing (or updating) the Resilience Plan.

It is good practice that the identified key processes and assets for their execution identified by the CI operator, as well as processes outsourced or resulting from interrelations with stakeholders, are included in the risk estimation process. Identifying risks arising from incidents involving unmanned systems can result in a change in the approach of the CI operator' or the CI system coordinator to risk assessment and perception of the CI security. In the process of analyzing threats and assessing risks, the extent of interrelations between the CI operator and the stakeholder is taken into account, as long as it is expressed in the cooperation or the draft agreement on the use of unmanned or anti-drone systems. The assessment of current or future cooperation should take into account the entities:

- affecting, being affected by, or which may consider themselves as affected by CI activities;

- performing subcontracting tasks in processes related to the operation of facilities, systems, equipment and services critical to the CI operator;
- public administration bodies.

The CI operator should also take into account recommendations following inspections or audits of operations carried out by public administration bodies and services performing tasks in the area of public order and security or public safety, as well as comments resulting from the arrangements made with regard to the resilience plan and responding during or after incidents.

2.5.4.5.2. Development of an internal document

In the process of analyzing the CI security, affecting the implementation of the public and business mission, the operator shall prepare an internal document the purpose of which is to prepare and present the reasonable grounds or lack of reasonable grounds for creating a system for preventing, responding to or mitigating the effects of threats from unmanned systems. The development of the document should be preceded by an assessment of the conclusions resulting from the process of identification and analysis of threats, which can be carried out according to the rules adopted and applied by the CI operator. In the next stage of works on identifying risks to the CI from unmanned systems at an unacceptable level, it is reasonable to follow the procedures adopted by the CI operator, the result of which should be a recommendation prepared for the management. When preparing a justification for the reasonable grounds for the development of such a system, the team recommending conclusions shall take into account the extent of the necessary changes in the organization and reference to the need for development and activities in the area of anti-drone systems.

The CI operator should assess the risk by at least:

a) assessing the likelihood of an identified threat;
b) assessing the direct (for the organization – operator) or/and indirect (for stakeholders) effects of the occurrence of the identified threat;
c) using a consistent and clear measure for describing probability and effects.

The document developed following the risk assessment should contain at least the following data:

a) the scope of processes and services identified as critical and covered by the CI protection;
b) processes directly or indirectly related to the risks posed by unmanned systems;
c) relations between the most important processes and services and the functions that support these processes and services, taking into account facilities and systems and other assets exposed to threats from an incident involving the use of unmanned systems.

The document should include visualization of the area and functional scope of the CI, using available graphic and electronic methods.

If the risk is non-existent or negligible, there is no need to prepare a separate document.

In the case of a positive recommendation for the development of a system to prevent, respond to or mitigate the effects of threats arising from incidents involving unmanned systems, the document should specify:

a) the scope of activities for which the requirements of the Standards are implemented;
b) the location of the facilities for which the system for preventing threats posed by unmanned systems is being implemented;
c) technical measures and organizational mechanisms to be provided to meet the requirements of the Standards;
d) principles for supervising the system developed, which should be adapted to the public mission carried out by the CI operator.

2.5.4.5.3. Principles for preventing threats posed by unmanned systems

The principles for preventing, responding to, or mitigating the effects of threats posed by unmanned systems, which are part of the CI operator's security policy, should be:

a) adequate to the threats posed by unmanned systems and to the results of the risk analysis;
b) developed in writing and approved by the management;
c) effectively communicated to the CI operator's personnel and, depending on the risk assessment, to service providers and subcontractors;
d) reviewed regularly for timeliness, relevance and adequacy, each time a risk assessment is carried out.

To achieve the goals set forth in the rules for preventing, responding to, or mitigating the effects of threats posed by unmanned systems, the CI operator should:

a) identify the elementary tasks for achieving individual goals,
b) provide the resources necessary to achieve the goals and perform the tasks,
c) identify measurable criteria for evaluating the achievement of goals and performance of tasks,
d) set deadlines for the achievement of individual goals and performance of individual tasks.

2.5.4.5.4. Planning

One of the main inputs necessary for the planning and operation of mechanisms to prevent threats posed by unmanned systems are the results of risk analysis. The CI operator should improve the existing risk management methodology, appropriate for the size and complexity of the organization, or implement a new one taking into account

the provisions arising from PN-ISO 31000 standard or another standard that follows from a recognized risk management standard.

Risk management methods that take into account the risks posed by unmanned systems to the CI should be integrated into the documentation of already functioning CI operator's security and management systems.

The risk management methods should identify internal requirements of the organization necessary for:

a) identifying threats associated with unmanned systems;
b) risk estimation methods;
c) planning how to handle risks;
d) assessing the results of risk handling and reassessing risks;
e) method to supervise the documented information that constitutes the results of risk management.

The CI operator should be prepared to identify and monitor the threat posed by unmanned systems on an ongoing basis by analyzing the following data:

a) results of the analysis of the business context;
b) results of the analyses of incidents involving unmanned systems already experienced by the operator,
c) information on events involving unmanned systems occurring within the scope of activities of other operators;
d) results of risk handling in the event that the applied risk handling triggers further threats as a consequence;
e) results of inspections and audits – internal and external ones;
f) reports and information obtained from personnel and stakeholders;
g) recommendations and requests of authorized services and institutions carrying out the public security mission;
h) information from other available sources.

The identified threats should be presented to the management in the form of documented information.

2.5.4.6. Principles of liability

The CI operator is responsible for:

a) developing principles for preventing threats posed by unmanned systems;
b) providing resources necessary to implement, maintain and improve threat prevention mechanisms;
c) indicating roles, powers and responsibilities of the personnel in the implementation of requirements for the prevention of such threats;
d) ensuring periodic review and improvement of the principles for preventing threats posed by unmanned systems;

e) revising existing risk management methods and criteria for acceptability of risks from unmanned systems, or developing and implementing a new method that takes into account the threats posed by unmanned systems;
f) promoting awareness of the severity of the threats posed by unmanned systems among the personnel and stakeholders;
g) continuously analyzing the context of the CI operator's operation in terms of the threats posed by unmanned systems;
h) participating in key activities to strengthen the security of the CI operator, including in the area of the operation of mechanisms to prevent threats from unmanned systems, as well as the implementation of findings from internal and external inspections and audits;
i) ensuring that requirements and mechanisms for preventing threats from unmanned systems have been incorporated into the business processes implemented by the CI operator.

2.5.4.7. Tasks and responsibilities within the CI operator's structure

The management should define the tasks, powers and responsibility for implementing, maintaining and improving the mechanisms for preventing threats from unmanned systems at the relevant levels of the CI operator's organizational structure, in a way that ensures efficient and effective implementation of the security policy.

It is necessary to define the method, procedure and form of reporting incidents to the management with regard to the effectiveness of existing mechanisms, procedures and instructions for preventing threats posed by unmanned systems.

2.5.4.8. Preparing the CI operators for responding to threats posed by unmanned systems

The CI operator's process of preparing for incidents involving unmanned systems should always begin with asking risk owners and managers of all security areas to indicate processes and services and assets which are critical to functionality, and whether the safeguards in place are sufficient to accept or tolerate risks to maintain the CI resilience and business continuity. The CI operator in the process of preparing for the response should:

1. confirm that the selected processes and services and designated assets, including facilities, systems, equipment as are the most important for the operation of CI;
2. identify possible incidents for the selected facilities, e.g., recognition of CI components, deliberate attack, accidental fall, regular uncontrolled entry;
3. identify potential threats affecting the CI and causing short or long-term interruption of the CI functionality based on representative event scenarios;
4. determine the likelihood of an incident involving unmanned systems for the selected processes, services, facilities, systems or equipment;

5. develop notification procedures and an action scheme for responders in the event of an incident;
6. develop stakeholder notification procedures;
7. prepare, on the basis of the conclusions of the risk assessment and its own organizational, technical and financial capabilities, mechanisms on the principles of securing the space surrounding the CI, along with the procedure for its shutdown, time limit or separation and marking;
8. prepare a plan for launching the process of securing the CI area with anti-drone systems capable of effectively detecting and neutralizing unmanned systems using the principles covered in subchapters 2.5.4.9. and 2.5.4.10.

The CI operator is prepared to record incidents and to prepare reports on events involving unmanned systems, which should include, at least:

1/ the person(s) and the security department responsible for the record of events;
2/ the date and times of the event and the locations or facilities involved;
3/ the type or model of the unmanned system and the direction from which it came;
4/ the entity reporting the incident;
5/ type of the event;
6/ consequences (effects) of the event.

The expanded version, the form "description of an incident involving an unmanned system" should record the following information:

1) location of the incident on a map or description of the location;
2) a description of the site (e.g., private property, railway siding);
3) type of the event (selection from a list, e.g., overflight/entry, hovering, presence/activity, cargo delivery/leaving, unintentional event/collision, intentional strike, sabotage (detonation/arson);
4) characteristics of the object/device (selection from the list by indicating, for example: type of propulsion: propeller, jet, rocket, free-running, free-floating, number of propulsions; single-propulsion, multi-propulsion, with wings, lighting, color, speed of movement, making sounds, other characteristics);
5) description of the cause of the event.

The CI operator is prepared to implement tests of the detection system, as long as a decision has been made to create anti-drone systems. General assumptions for the implementation of detection system testing on the example of unmanned aerial vehicles (UAV) should provide for the following tasks:

1. execution, so as to take into account various weather conditions, time of day, season of the year and different operating conditions of the protected facility;

2. UAV raids should be carried out from different directions and at different altitudes; in particular, consideration should be given to flying at altitudes below the height of obstacles present in the area the system is intended to protect;
3. during the tests, raids should be carried out in which several UAVs will be used simultaneously;
4. It is proposed that at least 5 raids, each from a different direction and at a different altitude, should be made as part of each test session;
5. test raids should be carried out with UAVs of various manufacturers and classes. It is recommended to use during the tests the UAVs of at least two different manufacturers and models that fall into the categories of C0, C1, C2, C3, C4, with a proprietary design design and a drone without any class assigned with a weight of less than 25 kg;
6. if the tests should not or cannot be performed at the CI site, then they should be conducted at another site with similar characteristics;
7. the tests should be carried out in a controlled environment and safe conditions, outside of the facility's operating hours or with the facility partially out of service, so that in the event of a malfunction of and loss of control over the UAV, it will not cause any threat to human health and life and loss of property;
8. the completion of the tests should be summarized in a report, which should include the data resulting from points 1–7, taking into account visibility and weather conditions, including temperature and wind strength, rain, snow, and reference to the number and type (model) of the drone, the direction, altitude and speed of its raid, the distance from the facility at the time of detection and also the effects of the system operation with conclusions.

2.5.4.9. Proposal of a method to evaluate the effectiveness of the unmanned platform detection system

Detection devices in CI protection systems are selected by evaluating the probability of detecting unwanted activity under given conditions.

For each detection device, the probability of detection of the unmanned platform under the given operating conditions and within the required time should be experimentally evaluated. The given operating conditions of the device are the conditions under which the device will operate, which means that the probability of detection of the unmanned platform is evaluated:

- → under various weather conditions (humidity, fog, rain, snow, no precipitation, high temperature, low temperature, day, night, no wind, strong wind, high noise environment, low noise environment, etc.);
- → in a given location (flat terrain, mountainous terrain, bushy terrain, forest, developed terrain, undeveloped terrain, paved road, dirt road, offshore storm conditions, no storm, etc.);

→ in the presence of external sources of electromagnetic radiation (radars for manned aviation, base transceiver stations (BTS), radio transmitters, etc.);

→ for various types of unmanned systems (multirotor, airplane, helicopter, unusually shaped vessel, wheeled vehicle, caterpillar vehicle, unmanned submarine, unmanned surface boat, etc.);

→ with various ways of carrying out the attack (high-altitude flight, low-altitude flight, high-speed flight, low-speed flight, straight-line flight, variable trajectory flight, driving on a paved road, driving on a dirt road, in the grass, in the forest, cruising in calm water, cruising in storm conditions, etc.);

→ with various competencies of physical security personnel responsible for operating detection equipment (e.g., well-trained employee, employee with no experience).

The detection probability evaluation can be carried out by counting the number of detections of a flying UAV per hundred overflights, or the number of detections of moving wheeled or caterpillar vehicles per hundred passes, or the number of detections of unmanned platforms floating under or on water per hundred passes.

These detections must be correct. The indications of instruments that misinterpreted the detection by recording objects other than unmanned platforms should be rejected. By taking into account the so-called false detections it will be possible to determine the actual number of correct detections.

Further considerations are carried out for the example of a flying UAV, but for vehicles or boats the probability will be evaluated on a similar basis.

In the case of one hundred detections out of one hundred UAV overflights under the given conditions, the probability will be 100%, if no single overflight is detected, the probability will be 0%. An additional parameter to be evaluated must be the detection time, called the required time for the purposes of the Standards. The required time is the time when a drone is detected early enough for dedicated procedures to be activated for a given type of incident, including an attack by an unmanned platform. The probability of detection of an unmanned platform under the given conditions and within the required time is expressed as P_{UX}, and *UX* is the x^{th} detection device.

The total probability of detection of an unmanned platform by a system that consists of N devices will be expressed by the formula:

$$P_{\text{tot}D} = 1 - (1 - P_{U_1})(1 - P_{U_2}) \ldots (1 - P_{UN})$$

Let us assume that an unmanned platform detection system is made of three detection devices. In the described example, in which the detection system is made of three devices, we will get three probabilities after testing $P_{U1}, P_{U2} oraz P_{U3}$.For the described system, the formula takes the following form:

$$P_{totD} = 1 - (1 - P_{U1})(1 - P_{U2})(1 - P_{U3})$$

Example: we consider a system made of three detection devices whose probability of detection determined for the given conditions and within the required time is: $P_{U1} = 0{,}33, P_{U2} = 0{,}65, P_{U3} = 0{,}54$. This means that for one hundred overflights these devices detected the drone: $U1 \rightarrow 33$, $U2 \rightarrow 65$, $U1 \rightarrow 54$ times. Thus, the calculated total probability of drone detection by such a system will be:

$$P_{totD} = 1 - (1 - 0.33)(1 - 0.65)(1 - 0.54)$$

$$P_{totD} = 0.89$$

or otherwise:

$$P_{totD} = 89\%$$

This result indicates that a system composed of Pu1, Pu2 and Pu3 devices will detect an unmanned platform with a probability of 89%, so it will detect 89 out of one hundred overflights. If the facility were protected by such a system, then for every one hundred overflights, eleven would go undetected and could successfully carry out an attack.

The task of the manager of the protected facility is to set a minimum threshold value of $P_{całkD}$ below which the system is considered ineffective. If the system is found to be ineffective, action should be taken to increase the value of $P_{całkD}$. This can be achieved by:

→ changing the detection conditions, for example, if the device does not perform well in an open area overgrown with bushes, the bushes can be cut down;

→ increasing the number of detection devices in the system, assuming that more devices operate on a different principle than those already used in the system;

→ replacing the device with the lowest probability of detection with a better one;

→ in the case of detection of wheeled or caterpillar vehicles, by using defeat devices;

or

→ in the event that there is no better model of the device on the market, preventive measures should be taken, as described further in the subsection, so as to prevent the attack from being launched.

Example: we assume that the unmanned platform detection system described above does not meet expectations and we want the probability of detection by the system to be higher. The probability of detection will be increased by adding other detection devices to the system, operating on a different principle than those already in the system.

So let us add devices with the probability of detecting unmanned platform under the given conditions and with the required time being: Pu4 = 0.50 and Pu5 = 0.60 respectively. Thus, the system under consideration is composed of five detection

devices. Therefore, the calculated total probability of platform detection by such a system will be:

$$P_{totD} = 1 - (1 - P_{U1})(1 - P_{U2})(1 - P_{U3})(1 - P_{U4})(1 - P_{U5})$$

$$P_{totD} = 1 - (1 - 0.33)(1 - 0.65)(1 - 0.54)(1 - 0.50)(1 - 0.60)$$

$$P_{totD} = 0.98$$

or otherwise:

$$P_{totD} = 98\ \%$$

This result indicates that a system with an unacceptable probability of detection of an unmanned platform, when supplemented with other detection devices, is very effective, and the total probability of detection increases by about 10% and is 98%. If the facility were protected by such a system then for every one hundred overflights only two would go undetected and could successfully carry out an attack.

When testing detection devices, it is important to keep in mind several principles that determine the effectiveness (and therefore probability) of detection:

1. detection devices must be absolutely independent of each other. Independence means that these devices must have different, separate power sources operating under normal conditions and power sources operating in the event of an emergency, they must have different, separate protection devices protecting against interrupted operation, and the detection devices must not affect each other in any way, such as by interfering with each other's operation through strong electromagnetic fields;
2. detection devices, as well as the entire detection system, must be periodically inspected. A periodic inspection results from the fact that any technical facility can be damaged which will dramatically reduce the value of $P_{całkD}$, perhaps even below the acceptable threshold value. The inspection also stems from the fact that every technical facility is aging. The detection system should also be tested whenever there is a change in system operating conditions. Such a change could be, for example, the construction of buildings or structures in the area of the protected facility;
3. the priority for the manager of a protected facility should be to ensure effective detection of an attacking unmanned platform, not the cost of building the system.

The unmanned platform detection system is considered properly constructed if the value of $P_{całkD}$ is higher than the permissible minimum threshold value.

When designing an unmanned platform detection system for a protected facility, detection devices should be selected so that their operation does not adversely affect the operation of equipment used in the protected facility. Negative impacts can include, for

example, electromagnetic fields emitted by the radar. If the field, its frequency and intensity, interfered in any way with the operation of the protected facility then such a detection device should be abandoned or measures should be taken to reduce the impact of the electromagnetic field on the equipment in the protected facility, such as through proper shielding.

2.5.4.10. Proposal for a method to evaluate the effectiveness of the unmanned platform neutralization system

The unmanned platform neutralization system should be made of devices that neutralize platforms in different ways, so that the probability of neutralization is sufficiently high. The use of devices that operate on different principles ensures that under all conditions the system will operate as intended, i.e. it will neutralize the platform. Devices that neutralize unmanned platforms should be selected for the system after evaluating their effectiveness, that is, the probability of neutralizing the platform under the given conditions and within the required time. The evaluation of the probability of neutralizing an unmanned platform should take place under the same conditions under which platform detection devices are evaluated. The effectiveness of neutralization should be evaluated by reference to:

→ various weather conditions (humidity, fog, rain, snow, no precipitation, high temperature, low temperature, day, night, no wind, strong wind, etc.);

→ location of the protected facility (flat terrain, mountainous terrain, bushy terrain, forest, developed terrain, undeveloped terrain, paved road, dirt road, marine storm conditions, no storm, population in the area, etc.);

→ conditions of external sources of electromagnetic radiation (radars for manned aviation, base transceiver stations (BTS), radio transmitters, etc.);

→ various types of unmanned systems (multirotor, airplane, helicopter, unusually shaped vessel, wheeled vehicle, caterpillar vehicle, unmanned submarine, unmanned surface boat, etc.);

→ ways of carrying out the attack (high-altitude flight, low-altitude flight, high-speed flight, low-speed flight, straight-line flight, variable trajectory flight, driving on a paved road, driving on a dirt road, in the grass, in the forest, cruising in calm water, cruising in storm conditions, etc.);

→ various competencies of physical security personnel responsible for operating detection equipment (e.g., well-trained employee, employee with no experience).

The neutralization probability evaluation can be carried out by counting the number of neutralizations of a flying UAV per hundred overflights, or the number of neutralizations of moving wheeled or caterpillar vehicles per hundred passes, or the number of neutralizations of unmanned platforms floating under or on water per hundred passes. Further considerations are made for the example of a flying UAV, but

for vehicles or boats, the way to evaluate the probability of neutralization will be the same.

The evaluation of the probability of neutralization of the unmanned platform for each neutralizing device can be carried out by counting the number of successful actions, as a result of which the platform ceases to pose a threat to the protected facility, per one hundred attempts. An additional parameter to be evaluated should be the required time needed to successfully neutralize the platform.

The required time should be considered to be the time when the platform is neutralized fast enough to be unable to successfully carry out an attack, e.g., fast enough for the unmanned platform to fail to carry an explosive charge close enough to the target for its explosion to cause damage, or fast enough for the unmanned platform to fail to capture imagery in an intelligence mission.

The probability of neutralizing an attacking platform by a device is expressed as P_{UY}, and UY is the y^{th} neutralizing device. The total probability of neutralization of an unmanned platform by a system consisting of N devices will be expressed by the formula:

$$P_{totN} = 1 - (1 - P_{U_1})(1 - P_{U_2}) \ldots (1 - P_{UN})$$

Example: we consider a system consisting of three neutralizing devices, whose probability of neutralizing an attacking unmanned platform determined for the given conditions and within the required time is: $P_{U1} = 0{,}50, P_{U2} = 0{,}65, P_{U3} = 0{,}64$. This means that for one hundred overflights these devices neutralized the platform: $U1 \rightarrow 50$, $U2 \rightarrow 65$, $U3 \rightarrow 64$ times.

Thus, the calculated total probability of platform neutralization by such a system will be:

$$P_{totN} = 1 - (1 - 0.50)(1 - 0.65)(1 - 0.64)$$

$$P_{totN} = 0.94$$

or otherwise:

$$P_{totD} = 94\ \%$$

This result indicates that a system composed of $P_{U1}, P_{U1} oraz P_{U1}$ devices will neutralize the platform with a probability of 94%, so it will detect approximately 94 per one hundred overflights.

To determine the probability of neutralization of the platform by the device, one should keep in mind several principles that determine the effectiveness (and therefore the probability) of neutralization:

1. neutralization devices must be absolutely independent of each other. Independence means that these devices must have different, separate power

sources operating under normal conditions and power sources operating in the event of an emergency, they must have different, separate protection devices protecting against interrupted operation, and these devices must not affect each other in any way, such as by interfering with each other's operation through strong electromagnetic fields;

2. neutralization devices, as well as the entire neutralization system, must be periodically inspected. A periodic inspection results from the fact that any technical facility can be damaged which will dramatically reduce the value of $P_{całkN}$, perhaps even below the acceptable threshold value. The inspection also stems from the fact that every technical facility is aging. The neutralization system should also be tested whenever there is a change in system operating conditions. Such a change could be, for example, the construction of buildings or structures in the area of the protected facility;
3. the priority for the manager of a protected facility should be to ensure effective neutralization of an attacking unmanned platform, not the cost of building the system.

The unmanned platform neutralization system is considered properly constructed if the value of $P_{całkN}$ is higher than the permissible minimum threshold value.

When designing a platform neutralization system for a protected facility, neutralizing devices should be selected in such a way that their operation does not adversely affect the facility or the people working in its vicinity. Such negative impacts can include, for example, the fall of an unmanned platform as a result of being shot down with a laser device on components of the facility equipment or people.

The kinetic energy of a falling platform is described by the formula:

$$E_k = \frac{1}{2} m v^2 \ ;$$

where: m – is the mass of the drone, v – the speed at which the drone hits the obstacle.

The consequence of a platform falling even with low kinetic energy can be injury or death to a person, and if it hits a technical facility, its operation can be interrupted. If the risk of a platform falling on people or systems were unacceptable, mitigation measures should be taken by, for example, building shields.

2.5.4.11. Summary

1/ The Standards have been prepared in a universal manner that allows adaptation and implementation of the requirements by any organization identifying threats from unmanned systems and wishing to improve security and ensure business continuity, including through the implementation of anti-drone protection.

2/ Meeting the Standards does not ensure full resistance to threats from unmanned systems; however, it demonstrates a high awareness of the nature of the threats and the

commitment of CI operators as well as owners and managers of facilities and areas subject to mandatory protection.

3/ Applying the Standards does not mean estimating risk only in the area of physical security, but also in the areas of personal security, technical security, including technological-process security, cybersecurity, and in protecting key processes and services supporting these and other areas of security from intentional or accidental interference by unmanned systems.

4/ The provisions of the Standard apply to drafted or amended contracts between the CI operator and the entity providing services with the use of unmanned or anti-drone systems.

2.5.5. Key recommendations for ensuring physical security:

1. Do not start building a physical security assurance system without first identifying the assets to be protected and the potential attacker.
2. The system is only as strong as its weakest link.
3. Technical measures to ensure physical security should be supervised by a human.
4. Motivation and competence of physical security personnel are critical.
5. Procedures that are not understood and applied do not protect.
6. Those authorized to use direct coercive measures must undergo regular training in this area.
7. A physical security assurance system unsupported by threat identification and analysis and risk assessment can be ineffective.
8. Physical attacks on critical infrastructure often lead to massive losses.
9. Periodic threat analysis and risk assessment in the CI security space requires reference to incidents involving unmanned systems.
10. Creating a system for preventing, responding to and mitigating the effects of the threats of incidents posed by unmanned systems requires expert opinion.
11. If the CI security assessments include unacceptable risks resulting from incidents posed by unmanned systems, the CI operator, in consultation with the CI system coordinator, shall determine the strategy and mechanisms necessary to build anti-drone systems.

2.6. Technical security assurance

Technical security assurance is a set of organizational and technical measures aimed at minimizing the risk of disruption to facilities, installations, technical or water equipment and services to ensure the continuity of their operation.

The basic and most effective way to ensure the technical security of CI is to comply with the legal acts, standards, operational regimes applicable to the infrastructure in question, as well as to implement the expert recommendations and findings of the risk assessment adopted and implemented by the CI system coordinator or CI operator.

The objective of technical security is to maintain the safe functionality of the relationship between employees and management and technology, including facilities, installations, equipment and maintenance and service – the environment, and to balance this relationship with the environment and climate.

The scope of technical security, within the framework of state and citizen security management, to ensure the smooth functioning of public administration bodies, as well as institutions and entrepreneurs, is due to:

1. protective role towards key services or supporting processes and services for them,
2. the functional uniqueness of the infrastructure, which is included in the uniform list of facilities, installations, equipment and services included in the CI in the various CI systems,
3. technical and organizational safeguards for the most important resources of the CI operator or system,
4. the magnitude of the effects, estimated on the basis of the adopted methods of analysis and assessment of the risk of a failure[13], serious failure[14], technical, chemical or environmental disaster, in particular, in terms of the effects on employees and society, the environment, national heritage assets and the country's economy.

The security of CI technical or water facilities depends on the processes carried out by the CI operator at plants, facilities or installations through all its stages and life cycles, requiring the involvement of employees at all levels applying the principles of proven practices of:

- technical,

[13] The state of inoperability of a facility, installation, equipment that prevents its operation.

[14] Serious failure – is an event, in particular an emission, fire or explosion, occurring during an industrial process, storage or transportation, in which one or more hazardous substances are present, leading to an immediate hazard to human life or health or to the environment, or to the occurrence of such a hazard with a delay; Article 3 point 23 of the Act of April 27, 2001 – Environmental Protection Law (Journal of Laws of 2001 No. 62, item 627).

- fire,
- chemical,
- technology and process,
- transportation,
- environmental,
- occupational security.

With these assumptions in mind, the security strategy for CI facilities should be based on the integration of activities derived from quality, environmental, security, business continuity and risk management systems, among others, in accordance with:

- PN-EN ISO 9001 Quality management systems,
- PN-EN ISO 14001 Environmental management systems,
- ISO 45001 – Occupational health and safety management systems,
- OSHA 1910.119 Process Safety Management (PSM),
- PN ISO 31000 Risk management,
- PN-EN ISO 22301 Societal security. Business continuity management systems,
- ISO 22313 Business continuity management systems – Guidance,
- BS 11200:2014 Crisis management – Guidance and good practice,
- NIST SP 800 – 34 Contingency Planning Guide for Information Technology (IT) Systems,
- HB 221 Business Continuity Management,
- Seveso III – Directive 2012/18/EU of the European Parliament and of the Council of 4 July 2012 on the control of major-accident hazards involving dangerous substances, amending and subsequently repealing Council Directive 96/82/EC.

Technical security regulations derive from EU and national legislation, the key requirements of which are contained in the Labor Code, Environmental Protection Law, Water Law, Construction Law, Nuclear Law, Geological and Mining Law, Energy Law, Act on fire protection, Act on the transport of hazardous goods, and others, as well as in the implementing regulations for these laws. Many regulations stem directly from the occupational safety and health directive, machinery directive, pressure directive, low-voltage directive, noise directive, electromagnetic compatibility directive, explosion prevention (atex) directive, prevention of serious failures directive (seveso III).

Technical security takes into account the impact of a number of risks affecting CI and the effects of which are unacceptable due to the possible own costs resulting from the possibility of interrupting the business mission, as well as causing social, economic, environmental and reputational (image) costs resulting from CI's public mission. Hence, it is important that the objective of risk management in the area of technical

security is to prevent losses[15], by maintaining or strengthening the resilience[16] of technical and organizational solutions that ensure the protection and functionality of the CI operator's infrastructure and individual CI systems. The priority of technical security management is to guarantee the safe use of the infrastructure at the required level, along with the fulfillment of its expected functionality, as well as the effective operation of independent safeguards in the event of an adverse event. Fulfillment of the expected requirements serves to prevent undesirable events, and in the event of their occurrence, providing guarantees for the activation of security systems designed to eliminate hazards, as well as for the protection and rescue of the CI operator's resources and to ensure the continuity of operation of key processes and services against the possible effects of accidents and failures.

Ventures in risk management and strengthening CI resilience by either the CI operator or process subcontractors or service providers to the CI operator integrate technical security issues in the following areas:

1) process security related to the use of hazardous substances and technology and process facilities, as well as services related to the provision of relevant products in the supply chain,
2) security of technical or water installations and equipment functionally integrated into the facilities and the area of the processes and services performed, as well as control over them,
3) occupational and health safety of employees – occupational security,
4) environmental security related to the adopted requirements under the EU climate law[17] and the state policy for environmental and climate protection,
5) critical infrastructure security related to adopted directives and EU and national security strategies.

Structures with their associated installations and equipment must be designed and built, and then operated in accordance with regulations and standards accepted for use, and in accordance with the principles and best practices of technical and engineering knowledge, ensuring, among other things:

1) meeting the basic requirements for:
    (a) load-bearing capacity and structural stability,
    (b) fire safety,

[15] loss – is an unreasonable change in the H-T-W-E (Human-Technology-Workspace-Environment) system, characterized by the loss of life or health of people or the destruction of other resources, the consequence of which may be the interruption of services or processes leading to the loss of a key service. Szopa T., Niezawodność i bezpieczeństwo [Reliability and safety]. Warsaw, 2016

[16] Resilience means a critical entity's ability to prevent, protect against, respond to, resist, mitigate, absorb, accommodate and recover from an incident –definition according to Article 2 of Directive (EU) 2022/2557 of the European Parliament and of the Council of 24 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC

[17] Regulation of the European Parliament and of the Council establishing the framework for achieving climate neutrality and amending Regulation (EU) 2018/1999 (European Climate Law) – (accessed January 22, 2021).

(c) hygiene, health and the environment,
(d) safety of use and accessibility,
(e) noise protection,
(f) energy savings and thermal insulation,
(g) sustainable use of natural resources.

2) operating conditions in accordance with the intended use of the structure and installations, in particular in terms of:
   (a) providing water and electricity and, as appropriate, heat and fuels, assuming efficient use of these factors,
   (b) disposal of wastewater, rainwater and waste,
   (c) the ability to maintain proper technical condition.
3) protecting the employees through the implementation of appropriate occupational safety measures under normal conditions and during emergency operations, e.g., fire, explosion, emission of a hazardous substance or other hazard,
4) protecting the structures listed in the historic register and structures under heritage conservation,
5) appropriate location on the building plot and compliance with the conditions arising from spatial development plans.

In facility security, a good practice is the approach that every design, production, import, construction, and operation of equipment, installations (and networks) should ensure reasonable and efficient use of fuels or energy while maintaining:

1) reliability of interaction;
2) operating and environmental safety, after meeting the requirements of environmental protection, occupational health and safety, fire protection, and the recommendations of experts and appraisers;
3) compliance with the requirements of the Polish Standards introduced for mandatory use or other recommendations resulting from technology of energy production and the type of fuel used.

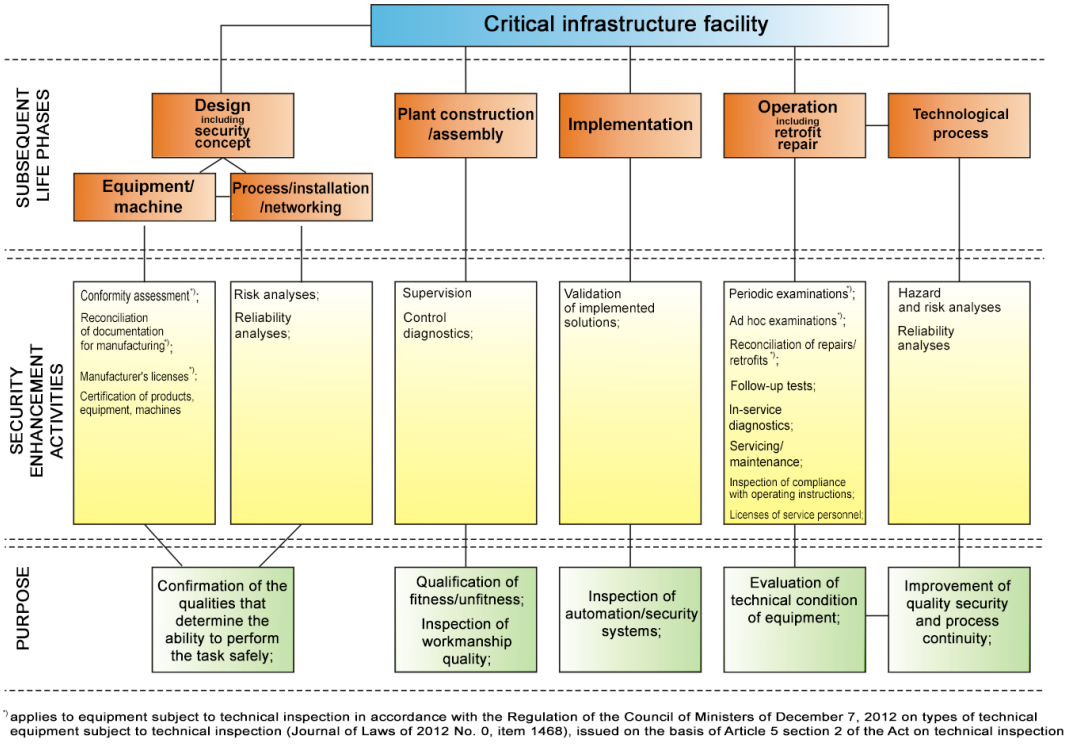


Figure 11 Selected activities to improve the security of critical infrastructure technical facilities in subsequent life phases.

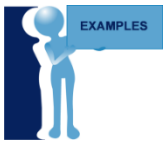
Technical equipment that poses a hazard by:

- expansion of gases under pressure different from atmospheric pressure,
- release of potential or kinetic energy when moving people or loads within a limited range (elevators, cranes, escalators),
- the spread of hazardous materials during their storage or transport <u>are covered by technical inspection!</u>

2.6.1. Four basic components of technical security assurance

A system that is resilient to disruption should be characterized by:

- continuous availability of the service or services,
- reliability,
- service capacity,
- security.



Depending on the situation and the operational importance of the equipment included in the CI security system, the following may additionally also be required: short repair times, the need for on-the-move replacement of critical components, good diagnostic strategies and an adequate spare parts inventory.

Availability

Until now, the priority in system design has been to use high reliability components, equipments and assemblies, which was supposed to be a guarantee of reducing the intensity of system failures. Nowadays, especially when designing new or retrofitting existing energy and fuel supply systems, communications and ICT systems, and water supply systems, great attention is also paid to solutions that guarantee service **availability**. Maintaining high availability requires careful planning and good service management.

The term **availability** means the ability to continuously use system resources at any time. **Availability percentages**, also called **readiness indicators** in the Polish literature, determine the design downtime and allow comparison of theoretical downtime resulting from the failure rate of a given system.

Table 6 Availability measurement[18]

Availability	Downtime	Downtime per year	Downtime per week
98%	2%	7 days, 7 hrs, 4 min	3 hrs, 22 min
99%	1%	3 days, 15 hrs, 32 min	1 hr, 41 min
99.8%	0.2%	17 hrs, 30 min	20 min, 10 sec
99.9%	0.1%	8 hrs, 45 min	10 min, 5 sec

[18] Source: Evan M., Hal S.: Blueprints for high availability, ed.2, Wiley Publishing, Canada 2003.

Availability	Downtime	Downtime per year	Downtime per week
99.99%	0.01%	52.5 min.	1 min.
99.999%	0.001%	5.25 min.	6 sec.
99.9999%	0.0001%	31.5 sec	0.6 sec

A system that causes a shutdown once a month and suspends the process for about 40 minutes has an availability of 99.9%. The same can be said for a system that initiates a shutdown once a year, but for about 9 hours. Assuming theoretically that it takes a maximum of 1 hour to repair a faulty component, the entire process line is usually doomed to many hours of downtime before all components are reconnected and start working.

The actual average downtime should be estimated already from the moment the damage is detected until the system is restored to the specified state of serviceability. It is often the case that this time is counted only from the moment of repair. It is therefore good practice to clearly define for a given CI operator what exactly is meant by the term of **MTTR (Mean Time To Repairs).**

Availability of electricity supply systems[19]

The values of required or expected availability for power supply systems are very high. A typical availability rate at a point of common connection is about 99.98% mainly because the network has redundancy. This means that it is possible to switch from one supply line to another in case of disruptions in line one or vice versa. The lines must be continuously monitored and operated. High levels of system availability are therefore determined by the correctness of the design concept, the correct choice of system architecture, the elimination of single points of failure, but are also the result of well-planned operational maintenance.

Reliability

Technical reliability is a property defined by the probability that a given piece of equipment or facility in the system will be operational within a certain interval, which can be time, but also, for example, the number of operations performed. Thus, the

[19] Source: Marshall G., Chapman D.: Jakość zasilania – poradnik [Power quality – a guide], published by Polskie Centrum Promocji Miedzi, Wrocław 2002.

parameter refers to the equipment included in the system. The basic indicators of system reliability are: **MTTF (Mean Time To Failure)** and **MTBF (Mean Time Between Failure).** Factors affecting reliability include:

- equipment redundancy,
- repair time,
- service strategy, such as continuous supervision, monitoring, and
- component selection, including: component quality and component selection program.

Service capacity

Regardless of how and when the technical infrastructure is used, the components that make it up are subject to constant wear and tear. In the case of large technical facilities, such as complex technological and power systems, transformers or pipelines, for example, maintenance and **overhauls** are important factors – affecting **availability** and **operational and reliability characteristics**, and together supporting operational **security.**

In the field of equipment and machine operation, in addition to post-failure overhaul, there are two ways of maintaining the technological infrastructure, which are:

- preventive planned overhaul,
- overhaul determined on the basis of an analysis of the technical condition.

The first way is mainly applied to such components of the system and when an overhaul interruption does not cause countable losses. Planned overhaul for equipment or machine performing responsible tasks, aims to minimize the risk of unplanned events and resulting losses, but it does not give 100% certainty of avoiding unexpected failure. In addition, often most failures occur right after an overhaul, such as as a result of personnel errors made during the overhaul. Overhauls, therefore, can be detrimental, as in an effort to restore the equipment to an ideal state, there can be a so-called "novelty effect," which means that many components fail early in the early stages of operation[20].

For functionally important components, it is a good practice to determine the optimal times to carry out their maintenance, i.e. to determine the timing and scope of overhaul based on knowledge of the technical condition and operating conditions. The prediction of their sustainability should then be supported by **comprehensive diagnostic studies**.

For long-running equipment, the global standards for ensuring security but also high availability have now become **RBM (Risk Based Maintenance)** and **RCM (Reliability**

[20] Source: Smith A. M., Hinchcliffe G.R.: RCM-Gateway to World Class Maintenance, Ed.1., Wyd. *Butterworth Heinemann, 2003.*

Centered Maintenance). Properly implemented, they serve to extend the service life of equipment.

Safety

Each facility, including its installation or equipment (e.g. machine, apparatus, building) requires various measures to protect and maintain the level of security, which in a documented manner should regulate the maintenance of their reliability and confirm the supervision of their functionality.

Any properly and safely designed CI facility must take into account applicable standards and laws, contained in, among other things:

- Regulation of the Minister of Infrastructure of April 12, 2002 on technical conditions to be met by buildings and their location (Journal of Laws of 2022, item 1225),
- Regulation of the Minister of the Interior and Administration of June 7, 2010 on fire protection of buildings, other civil structures and areas (Journal of Laws of 2022, item 1620),
- Regulation of the Minister of the Interior and Administration of July 24, 2009 on fire water supply and fire roads (Journal of Laws No. 124, item 1030),

However, meeting the requirements set forth in the regulations means meeting only **the minimum requirements**. When designing the implementation of new processes, there may be a lack of national regulations (e.g. for the chemical industry). This forces design engineers to use regulations "by analogy".

To supplement local regulations, it is good practice to use international regulations, standards or guidelines. Increased oversight by fire and occupational health and safety experts and verification of the correctness of the design – for example, by performing a hazard analysis and security assessment and modeling the consequences of potential failures – are also becoming crucial at the design stage.

Security of critical infrastructure in terms of lightning protection[21]

Performing a risk analysis at the design stage in accordance with the requirements of PN-EN 62305-2 makes it possible to assess the hazard to the facility from lightning and, as a result, select appropriate protection measures to reduce the existing risk to an acceptable level.

[21] Source: PN-EN 62305-2:2012 Protection against lightning – Part 2: Risk management.

At the design stage of technological equipment or installations, two closely related issues should be considered:

- proper implementation of the process flow,
- ensuring security in normal operating states and emergency states.

This means that in the structure of technical objects there are – in addition to the **functional system** necessary for the implementation of the processes and tasks for which the facility is intended – **security systems,** including **protection automation**. Their task is to prevent disruptions, resulting from the operation of the facility, from turning into failures and disasters, and to reduce the negative effects of these events, if they already occur. The primary function of security systems, which can also be integrated with control systems, is the **monitoring** of relevant operating parameters and **technical diagnosis**[22] to detect possible damage or irregularities. Diagnostic actions are often combined with optical or audible **alarms** and process **interlocks**.

Technical standards for **security systems** do not require the implementation of a specific technology, levels of redundancy or time intervals at which to perform, such as proof testing. However, in terms of general requirements for protection automation equipment, resulting from reliability considerations, it is mentioned the use of:

- a minimum of two independent types of protection, each of which should work with separate measuring, control and shutdown circuits;
- hardware and software means for **self-diagnosis**, i.e. realization of continuous control and self-testing functions[23].

Operators of critical infrastructure facilities should be able to document that the technological processes they implement are designed and operate in a safe manner. The systems of security and limitation of the effects of failures used at facilities usually have a multi-layered structure, resulting, for example, from the complexity of the process, while always fitting into the model of three independent layers of protection (*Table 7*):

(1) prevention,
(2) limitation,
(3) counteraction.

[22] Source: Zbrowski A., Kozioł S.: Monitorowanie i diagnozowanie procesów i obiektów technicznych w systemach zapewnienia bezpieczeństwa technicznego, *Nauki humanistyczne i społeczne na rzecz bezpieczeństwa* [Monitoring and diagnosis of technical processes and facilities in technical security assurance systems, *Human and social sciences for security*], No. 1, 2011, pp. 59–68.

[23] Source: Orzyłowski M.: Przemysłowe systemy informatyczne [Industrial IT systems], Part 9. Autodiagnostyka przemysłowych systemów sterowania [Self-diagnosis of industrial control systems], 2003.

Table 7 Security vs. three independent layers of protection[24]

THEORY	PRACTICE
Preventive protection level, the so-called control layer **Objective: prevention of failures**	Ex execution (if required) emergency power and backup systems basic measurement and control system (BPCS – Basic Process Control System, DCS – Distributed Control System) process supervision system (e.g. SCADA – Supervisory Control And Data Acquisition) process and system alarms actions of operators and controllers, e.g. manual correction of the system internal procedures
Limiting protection level, the so-called security layer **Purpose: protection of the facility and employees from the effects of failures**	SIS – Safety Instrumented Systems, such as – ESD – Emergency Shutdown Systems – SSD – Safety Shutdown Systems operator responses to critical condition alarms emergency discharge systems, safety valves gas leakage and fire detection systems barriers, enclosures, trays, etc.
Counteracting protection level, the so-called mitigation layer **Objective: counteracting the effects of failures on people and the environment**	firefighting and neutralization systems (e.g. water systems, foam systems, water curtains, hydrants), personnel and rescuers at facilities (e.g. chemical rescue) facility/state fire departments evacuation medical assistance

The hallmark of a multilevel protection system is the sequential activation of successive layers of protection after the previous layer malfunctions. The actual security level of a facility therefore depends on the condition and proper operation of all layers of protection. The selection of appropriate types of safeguards for the prevention, limitation and counteraction layers should be determined based on the specifics and

[24] Source: Developed based on recommendations from the Office of Technical Inspection (UDT).

types of hazards. Some layers of limiting the effects of failures may be single-purpose, i.e. they will counter only specific hazards.

The tray will not prevent the formation of a vapor cloud if the liquid tank overflows, but it can be effective in preventing the working medium from seeping into the ground.

2.6.2. Guidelines for installations, equipment and machine in operation

During long-term operation, numerous changes in the process and operating conditions are observed, which, combined with random events caused, for example, by human error or environmental effects, significantly affect the functionality, reliability and safety of the facility.

In order to prevent potential failures and ensure the long-term operation of a given CI facility, it is advisable to successively conduct a **comprehensive assessment of technical condition** based on safety analyses and individually dedicated testing and measurement programs.

Hazard identification requires an analysis of historical data and past events, but also takes into account future projections based on knowledge about the facility.

For facilities that have been in operation for a long time, especially when there has been a change of ownership of the facility several times, it may turn out that:

- technical documentation (design/as-built/license documentation) of facilities is incomplete or outdated (e.g., drawings do not reflect the actual state of piping layout, strength calculations for pressure equipment are missing, etc.),
- there are no records of operating times, number of shutdowns and start-ups,
- conducted assessment of the facility condition is based only on visual inspection of accessible areas,
- the scopes of tests and measurements performed are incomplete or include randomly selected components.

In such a case – in the first instance – it is advisable to conduct an inventory, in terms of verifying the data that should be collected for operational safety. The information collected will also be useful in conducting risk assessments. The inventory is usually carried out without the participation of a broad team of experts.

In the second stage, based on the information gathered during the preliminary activities, further tasks can be carried out in two tracks, and will consist of:

- determining of equipment or components to be assessed in detail, identification of degradation mechanisms and diagnostic testing;
- identifying hazards, taking into account their type and location, and performing risk assessments.

A basic prerequisite for performing a proper operational safety assessment of a facility will be to appoint qualified teams and decide on the methodology:

- diagnostic and analytical tests,
- development of risk assessments.

Equipment subject to technical supervision by the Office of Technical Inspection.

The diagnostic testing program is developed individually for each equipment or component, taking into account the scope of testing and the criteria for evaluating the results. For technical equipment subject to technical supervision, it is required to agree on the scope of testing with the locally competent branch of the Office of Technical Inspection.)

The final expected result *after* the application of a comprehensive assessment of the technical condition of the CI facility, based on diagnostic testing and risk analysis, is to obtain proof that **all technical and functional conditions are met for the facility to ensure secure and long-term operation.**

2.6.3. General requirements for civil structures

Structures with their associated installations and equipment must be designed and built, and then operated in accordance with regulations and standards accepted for use, as well as results from risk assessments, and in accordance with the principles and best practices of technical and engineering knowledge, ensuring, among other things:

2) meeting the basic requirements for:
   (d) load-bearing capacity and structural stability,
   (e) fire safety,
   (f) hygiene, health and the environment,
   (g) safety of use and accessibility,
   (h) noise protection,
   (i) energy savings and thermal insulation,
   (j) sustainable use of natural resources;
3) operating conditions in accordance with the intended use of the structure and installations, in particular in terms of:
   a) providing water and electricity and, as appropriate, heat and fuels, assuming efficient use of these factors,
   b) disposal of wastewater, rainwater and waste,
   c) the ability to maintain proper technical condition,

6) protecting the employees through the implementation of appropriate occupational safety measures under normal conditions and during emergency operations, e.g., fire, explosion, emission of a hazardous substance or other hazard,
7) protecting the structures listed in the historic register and structures under heritage conservation,
8) appropriate location on the building plot and compliance with the conditions arising from spatial development plans.

In facility security, a good practice is the approach that every design, production, import, construction, and operation of equipment, installations (and networks) should ensure reasonable and efficient use of fuels or energy while maintaining:

4) reliability of interaction;
5) operating and environmental safety, after meeting the requirements of environmental protection, occupational health and safety, fire protection, and the recommendations of experts and appraisers;
6) compliance with the requirements of the Polish Standards introduced for mandatory use or other recommendations resulting from technology of energy production and the type of fuel used.

Structures must be used in a manner consistent with their intended use and environmental protection requirements, and should be maintained in good technical condition, not allowing excessive deterioration of their operational characteristics and technical efficiency.

The owner or manager of a structure, especially a building, is obliged to:

(1) maintain and operate the facility in accordance with the above-mentioned principles;
(2) ensure, exercising due diligence, the safe use of the structure in the event of external factors affecting the structure, related to human activity or forces of nature, such as lightning, seismic shocks, strong winds, intense precipitation, landslides, ice phenomena on rivers, seas, lakes, and water reservoirs, fires or floods, resulting in damage to the civil structure or an imminent threat of such damage, which may cause a threat to human life or health, property safety or the environment.

Civil structures should, during their use, undergo inspections by the owner or manager, including:

(1) periodic inspections, at least once a year, involving the assessment of the technical condition of:
    a) components of the building, structures and installations exposed to harmful atmospheric influences and destructive factors occurring during the use of the structure,

b) installations and equipment supporting environmental protection,
c) gas installations and flues (smoke, flue and ventilation),

(2) periodic inspection, at least once every 5 years, involving the assessment of the technical condition and suitability for use of the civil structure; this inspection should also include an examination of the electrical and lightning protection system in terms of the state of efficiency of connections, fixtures, protections and means of protection against electric shock, insulation resistance of wires and grounding of installations and apparatuses,

(3) periodic inspection, at least twice a year, by May 31 and November 30, for buildings with the footprint area exceeding 2000 m^2 and other civil structures with a roof area exceeding 1000 m^2; the person carrying out the inspection is obliged to immediately notify the competent authority in writing of the inspection,

(4) safe use of the structure each time there are external factors affecting the structure, related to human action or forces of nature.

The inspections are carried out by persons holding construction licenses in the relevant area of expertise.

Inspections of the technical condition of electrical, lightning protection, gas and refrigeration installations may be carried out by persons with the qualifications required for supervision of the operation of equipment, installations and power and gas networks.

The owner or manager of the civil structure is required to keep the construction documentation, as-built documentation, and other documents and decisions related to the building for the entire duration of the structure's existence, as well as, if necessary, instructions for the operation and use of: the structure, installations and equipment related to the structure, as well as design studies and technical documents of construction work performed in the structure during its use.

The owner or manager is obliged to keep, for each building and civil structure that is not a building, the design of which is subject to inspection, a civil structure log book, which is a document intended for records of tests and inspections of the technical condition, repairs and alterations carried out, during the period of use of the civil structure.

In the event of a construction disaster in a civil structure under construction, demolition or use, the Construction Site Manager (Lead Discipline Engineer), owner, manager or user is obliged to:

(1) organize emergency assistance to the injured and prevent the escalation of the consequences of the disaster,

(2) secure the site of the disaster from alterations that would prevent the investigation of the causes of the construction disaster by the competent construction supervision authority. The above activities shall not be performed in the case of saving lives or preventing the spread of the consequences of the disaster. In these cases, the post-disaster condition and the alterations made to it must be described

in detail, with the locations of the alterations marked on sketches and, if possible, on photographs,

(3) immediately notify of the disaster:

a) competent authority,
b) the locally competent prosecutor and the police,
c) the investor, the investor's representative and the design engineer of the civil structure, if the disaster occurred during construction,
d) other authorities or organizational units with jurisdiction over the disaster by virtue of specific legislation.

The investor, owner or manager of the civil structure after the completion of the investigation into the causes of the construction disaster is obliged to immediately take the necessary measures to remove the consequences of the construction disaster.

2.6.4. Fire protection

The basic activities for fire protection of critical infrastructure are:

- compliance with fire safety technical, construction, installation, and technological requirements,
- equipping buildings, civil structures or areas with hand-held fire-fighting equipment and fire-fighting equipment as required by law:
  - stationary and semi-stationary firefighting and safety equipment,
  - equipment included in the fire alarm system and voice alarm system,
  - installations of egress lighting and emergency lighting,
  - fire hydrants, landing valves,
  - pumps in fire pumping stations,
  - fire shut-off dampers,
- smoke extraction equipment, fire doors and fire shutters, as long as they are equipped with control systems,
- relief equipment and explosion pressure protection,
- ensuring that any fire-fighting appliances and portable fire-fighting equipment are maintained and repaired in a manner ensuring their proper and reliable functioning,
- ensuring the safety and evacuation capability for individuals on critical infrastructure premises,
- preparation of buildings, civil structures or critical infrastructure areas for rescue operations.

In addition to technical measures, organizational regimes shall be introduced, i.e.:

- familiarizing employees with fire safety regulations,
- determining procedures for handling fire emergencies, natural disasters or other local hazards.

In addition, fire protection of critical infrastructure shall include:

- the use of fire alarm systems equipped with signaling and alarm equipment,
- taking into account fire protection requirements during land development and utility connection to building site infrastructure,
- connecting of the fire alarm system to the premises of the State Fire Service headquarters or a facility designated by the locally competent district (municipal) commander of the State Fire Service,
- providing design documentation that includes fire protection requirements,
- the obligation of the manufacturer of machine, equipment and other products and the purchaser of foreign licenses or imported machine, equipment and other products to meet fire protection requirements,
- commissioning a new, reconstructed or renovated building, structure, site, machine, equipment, installation or other product after ensuring compliance with fire protection requirements and confirming that the equipment, fire and rescue tools, and firefighting agents provide effective fire protection,
- prohibiting activities that may cause fire or other localized hazards, facilitate their spread, or obstruct rescue operations or evacuation,
- maintaining fire routes in a condition that allows their use by vehicles of fire protection units,
- ensuring proper access to buildings and structures for emergency units,
- implementing fire safety plans,
- compliance with the rules for the use or storage of fire-hazardous materials,
- provision in the structures of equipment and installations for the supply of water for firefighting purposes,
- use of stationary firefighting equipment, permanently connected to the structure,
- the use of a voice alarm system to broadcast warning signals and voice messages for the safety of the structure occupants.

Evacuation is one of the fundamental measures to protect the life and health of people and animals, as well as to save property, in the event of a fire. Safe evacuation of people from structures is possible while maintaining the appropriate technical and construction conditions for evacuation routes and interior components. The conditions and organization of the evacuation of people are specified in the fire safety manual, and practical methods for verifying them are carried out through exercises. Evacuation can also be preventive.

It is important that fire protection systems are designed, installed, maintained and operated to the highest quality standards. It is recommended that individuals providing services in this area have the appropriate qualifications and competencies.

The correctness and reliability of the operation of technical fire protection systems, particularly fire alarm systems, are crucial for maintaining the fire safety of the protected structure. It is good practice for individuals providing services in the design, installation,

maintenance and operation of fire protection systems to have completed a course or training (in the relevant equipment area) from a recognized independent training institution.

Reference to the competence and qualification requirements of individuals performing services in the field of technical security systems is derived directly or indirectly from laws, standards, technical specifications and industry standards. Reference to the requirements is contained in the Act on fire protection, the Regulation of the Minister of Interior and Administration dated September 17, 2021 on coordinating the land or site development plan, building plans and specifications, technical design and fire protection system design to ensure compliance with the requirements of fire protection (Journal of Laws of 2021 item 1722 as amended), Regulation of the Minister of the Interior dated April 12, 2002 on the technical conditions to be met by buildings and their location (Journal of Laws of 2022, item 1225, as amended), technical specification PKN-CEN/TS 54-14:2020-09 Fire alarm systems – Part 14: Guidelines for planning, design, installation, commissioning, use and maintenance, as well as in EN 16763 Services for fire safety systems and security systems, and in industry standards.

2.6.5. Technical measures to reduce dependence of CI operation on external services

For structures where critical infrastructure components are located, the highest requirements for reliability of power supply and access to utilities should be adopted.

Meeting the above requirements can be achieved by:

- feeding from two independent power systems, water supplies and communications or data networks. The duct work should be placed underground and lead to various locations in the building,
- power supply to the installation by backup-stabilizing equipment – the capacity of the battery bank should be selected taking into account all the pieces of equipment that require backup,
- supply backup power to the structure from a generator set – the power of the set should be sufficient to supply all pieces of equipment requiring backup, taking into account the nature of the load from these pieces of equipment,
- own water intake – the capacity of the intake should take into account the nature of the activity and the minimum requirements to sustain or safely shut down technological processes. Water sources should be separated from other components of the infrastructure,
- water (gas, diesel, etc.) tanks, the capacity of which should take into account the minimum requirements to sustain or safely shut down technological processes,
- an annually reviewed emergency supplier plan.

Power and utility access reliability requirements is best considered as early as the infrastructure design process. Addressing these requirements at an early stage will improve CI security with the least amount of effort and cost. The situation is similar in the case of repairs or modernizations.

2.6.6. Technical measures to ensure continuity of CI operations

Ensuring that operations can be continued in a backup location is the best way to protect against threats. However, the use of this method depends on the technical and economic capabilities of the organization.

In the absence of a backup location, redundancy of critical infrastructure components is advisable. This applies in particular to ICT system structure equipment, such as servers, routers, and switches. Nevertheless, it is the risk assessment of disruption to CI that should be the basis for deciding which components of the organization's infrastructure should be duplicated. Redundancy should be both logical and physical.

Heating, ventilation, air conditioning (HVAC) systems (if used) should be planned so that they can operate in internal air recirculation mode, without exchanging air with the

environment. This will provide protection against unwanted, external contamination that may occur in the event of unforeseen incidents, such as fire, harmful chemical dust or biological agents. The level of safety can be increased by installing detectors that monitor air for the presence of chemical, biological, radioactive and other contaminants. Air conditioning systems, which are essential for the proper operation of the serviced technological equipment, should be designed with one backup air conditioner and at least one full refrigeration circuit.

2.6.7. Technological and process safety

Technological and process safety is the state of technology, equipment, storage, transport-logistics, and organizational design and operation of processes that guarantees effective prevention of the release of hazardous substances or energy into the working environment and the natural environment, and limits and mitigates the consequences of such releases (emissions).

In technological and process safety, each hazard is characterized by a specific hazard factor[25], which generally include the properties of substances and processes, as well as possible technical failures and human behavior, which are the source of potential losses

25 Technological and process risk factor is a parameter/magnitude that characterizes the process hazard.

to workers, property and the environment, as well as local communities depending on spatial conditions.

In technological and process safety, a hazard defines the state of a production process occurring with chemical substances/energy, whose natural physical, chemical or biological properties, are the starting component for assessing improper process conditions, the occurrence of an accident, or erroneous organization and management decisions resulting in undesirable effects and losses.

Among the most significant impacts, with the greatest losses, especially in industry, transportation or storage of hazardous products, are incidents involving hazardous substances or substances whose hazardous characteristics to life, health and the environment arise only as a result of an accident.

2.6.7.1. *Selected risk groups and factors in technological and process safety*

Significant risk factors[26] in the technological and process area include:

- processes involving high and low pressure,
- processes involving liquefied gases under pressure or in a cooled state,
- processes involving superheated liquids,
- processes occurring within explosive mixtures and in oxygen-enriched mixtures,
- oxidation processes of combustible substances,
- grinding and milling processes,
- thermal expansion and material brittleness,
- static electricity,
- hazardous chemical properties of substances/products,
- chemical reactivity arising from the reaction of two or more hazardous substances or from conditions that allow a low-hazard substance to be transformed by a reaction into a hazardous substance,
- exposure to toxic, explosive, fire-related factors, associated with energy flow, thermal radiation or low temperatures, noise, oxygen deficiency, or chemical, biological, radiological and nuclear factors,
- human factors – inexperience and insufficient knowledge, low qualifications, lack of competence, low awareness of hazards and risks, or low execution or management culture in the field of process safety maintenance.

In Polish industry, it is recommended to classify hazards into 5 groups. While these do not cover all possible categories and divisions in technological and process safety, they

[26] A. S. Markowski, Bezpieczeństwo procesów przemysłowych [Industrial process safety], Łódź University of Technology Publishing House, Łódź 2022 – chapter on process risk management in industry.

prove effective in practice when identifying hazards and conducting risk analysis, particularly:

1. Process hazards that are related to the conditions of ongoing process operations involving the following risk factors, in particular:
   - high/low temperature,
   - high/low pressure,
   - overfilling,
   - explosion or internal fire,
   - chemical incompatibility.
2. Material hazards that are related to the properties of chemicals or the type of energy used including the following risk factors, in particular;
   - chemical structure and oxygen balance of the substance,
   - flammability,
   - explosiveness,
   - reactivity,
   - toxicity,
   - corrosiveness,
   - thermal instability,
   - self-polymerization tendency,
   - phase transition capability,
   - exothermicity,
   - dispersion capability,
   - ecotoxicity.
3. Technical hazards that are related to process apparatus and equipment including the following risk factors, in particular:
   - loss of integrity or equipment (leakage),
   - mechanical, e.g., stress, material defects, erosion, vibration,
   - process automation failures,
   - equipment failures of process safety systems,
   - lack of testing,
   - design errors in the location, structure of installations, arrangement, selection, and applied safety barrier principles,
   - failures in the supply of auxiliary media (e.g., steam, electricity).
4. Organizational risks that are related to deficiencies in security management processes involving the following risk factors, in particular:
   - lack of a process safety policy,
   - lack of risk management mechanisms,
   - lack of implementation of risk analysis and assessment (if used) for change management and other safety management mechanisms,
   - inadequate operational (work) procedures,

- human errors due to lack of knowledge, training, skills at the expected level, violation of safety procedures and rules, or due to negligence,
- low maintenance, servicing and upkeep of process plant and equipment,
- lack of exercises and other forms of verification of safety and emergency rules,
- inadequate management structure in emergency prevention and response processes,
- low safety culture and an inadequate communication system in process safety management,
- lack of response plans for accidents and failures, as well as for business continuity and recovery of process infrastructure,
- low competence of key personnel in relation to high safety standards.

5. External risks, which are related to the possible influence of external factors including the following risk factors, in particular;
   - reduction or interruption of essential services and product supplies that ensure the continuity of operations and functionality of industrial processes,
   - external fire, explosion or emission of a hazardous substance or the domino effect resulting from their consequences,
   - danger from forces of nature (flooding, high winds, snow or rainfall, lightning, high or very low ambient temperatures, epidemics),
   - a low culture of cooperation between the public administration and companies implementing industrial processes,
   - low competence of emergency services and crisis management structures in preparing for and responding to the consequences of a major industrial accident,
   - cyber attack, sabotage or other forms of intentional criminal activity,
   - errors in legal regulations.

The level of process risk depends on many different interrelated factors and conditions, whose complex combination ultimately leads to a failure or industrial disaster (major accident). Some of these factors, on their own, do not pose a threat, but when combined with others, they significantly increase or create risks that can ultimately lead to the materialization of the hazard and the occurrence of losses. Practical examples of such risks are the results of analytical work in high and increased risk plants (HRP and IRP)[27], as well as in many sub-threshold plants[28].

[27] Environmental Protection Law – chapter on Prevention of Major Accidents (Seveso III) - according to data from the Chief Inspectorate of Environmental Protection, as of December 31, 2021, there were 477 HRPs and IRPs registered in Poland.

[28] This is the usual name for plants that use significant amounts of hazardous substances, but are not included in the HRP and IRP referred to in the Environmental Protection Law – according to the State Labor Inspection data, there are about 750 such plants in Poland, while according to the National Headquarters of the State Fire Service of Poland data, there are about such 1,100 plants in Poland.

In process installations, there are usually a considerable number or a very large number of factors that determine the level of process risk, with special significance attached to:

- the type of substances used, their hazardous properties, and their quantity,
- operational conditions for the process,
- installation location,
- reliability (unreliability) of personnel, including their competence,
- proper design in terms of functionality and resilience, as well as operation and maintenance management,
- risk and safety management system.

2.6.7.2. *Assessment of the process system security assurance*

The assessment of the process system security assurance, regardless of its sector of application, is performed by applying two basic approaches:

1) based on conformity assessment, and
2) based on an assessment of the risk of an accident or major accident.

Every approach to ensuring the security of a process system requires documented organizational and technical measures on the part of the CI operator, in particular:

1. System characteristics (process nodes).
2. Threat identification
3. Selection of representative accident and emergency events.
4. Assessment of consequences from event scenarios from a list of representative accident and emergency events.
5. Probability assessment.
6. Risk calculations.
7. A risk assessment that guides through options for reducing the likelihood and/or consequences of accidents to optimize risk management.

Before launching the risk management process, it is worth doing some solid preparatory and planning work, requiring teamwork and approval by the CI operator of the decisions on the course of the various components related to the identification of threats, and then to the analysis, assessment and handling of the process risk. It is also worth reviewing the previous approach to risk analysis and assessment, provided that the risk management process has been implemented cyclically in technology and process security.

As part of the preliminary works the number of systems, the relevance and impact of factors on their security and process continuity are inventoried, the time required to perform a risk assessment and the time required for discussions and recommendations for individual systems or process nodes, and ultimately for the entire plant are estimated.

The risk analysis begins with the collection of data on the properties of the chemicals used (e.g., on the basis of safety data sheets) and a thorough study of historical data on the occurrence of incidents and accidents for the system under study at the CI operator and at other entities (organizations), with a similar scope of activity. As part of these works, the design assumptions and all documents that describe and illustrate the characteristics of the system or individual process nodes and the surrounding area are analyzed, and it is possible to collate and compare the requirements and standards related to its security, including protection systems, as well as data on the substances used with their classification and quantities, the location of the system, an assessment of ambient conditions, weather conditions, and a description of the technology with accompanying diagrams. The analytical process involves visits to the system and a summary of the works done so far from the characteristics of the system, along with a clarification of the plan for further actions as part of the continuation of the hazard analysis and risk assessment process.

The first stage of the analysis identifies the sources of internal and external threats, and identifies possible events that initiate the sequence of emergency events, including causes and effects. Various qualitative methods are used at this stage of the works, the most common of which are the HAZOP or PHA comprehensive methods. It is also possible to use other methods such as simplified “What-if?” method or checklists.

The HAZOP method is universal in nature and is most commonly used in industry, as it is based on identifying all potential factors of threats and accidents and other losses occurring in process systems due to deviations from the normal, assumed operating conditions of a given system or equipment. Two typical features that characterize this method are: the systematic use of a set of keywords and an analytical team. When using this method, it is necessary to:

1) develop a worksheet;
2) divide the system into nodes;
3) determine the depth of analysis, i.e., the depth of consideration of causes and limiting operational parameters for each process node, as well as the type and amount of chemical they contain;
4) identify the type of process deviations relevant to each system node;
5) develop criteria for the selection of representative emergency events (RZA), either through a selection matrix or a ranking matrix (CI operator’s decisions);

6) conduct a HAZOP analysis and, based on it, develop a list of emergency events (LZA) and then a list of representative emergency events (LRZA).

The PHA method focuses on the hazard factors associated with the release of hazardous substances with reference to the entire system or separated nodes of the system. Once the worksheet is accepted, the causes, possible effects and type of protection systems either in place or to be designed are determined one by one for each type of threat. In the next step, the category of frequency of occurrence of specific effects and the category of magnitude of effects are estimated. This activity identifies the risk category or value, which is preceded by the selection of a matrix.

The list of emergency events (LZA) can be simplified to a so-called list of representative emergency events, meaning that the release involves the same substance and one type of instrumentation operating with similar operational parameters, as well as that it can represent similar events of this type, for the same test section. It is important to adhere to the following principles when allocating an emergency event to representative emergency scenarios:

1. Select ranking methods by risk level or threat level.
2. The principle of combining similar events involving the same substances and the same or similar operating conditions.
3. The reliability principle based on the possibility of occurrence of a given emergency event.

Each event is analyzed to determine the mechanism of origin and development of the event. Representative emergency events are subjected to analyses, preferably on a "brainstorming" basis, in order to select representative emergency scenarios (events) – RSA. Various analytical techniques are used in this regard, i.e. fault trees (FTA), event trees (ETA) and the bow-tie method. The execution of tasks in the risk analysis process provides knowledge of: what can happen, how it will happen and what the consequences will be, which is a key part of the process for preparing risk management optimization. For analyzing emergency scenarios, the bow-tie is the most recommended method because it:

- illustrates the relationships between initiating events, transitional events (which determine and enable scenario development), security systems (barriers) that perform relevant security functions, and other control factors;
- combines fault tree (FTA) and event tree(ETA) methods.

The stage of impact analysis and assessment does not depend only on the characteristics of the properties and release of hazardous substances, but also on the speed and efficiency of the operation (counteraction) of the protection system, i.e. the internal technical and organizational solutions. The effectiveness of countermeasure systems is also affected by the identification of factors that determine an undesirable event, such as the characteristics of the ignition source, the spaces in which the physical effects

occur, or the structural characteristics of facilities, such as structures or buildings. Determining the magnitude of effects and the extent of releases (i.e., hazard zones) is the goal of the analysis of physical effects and impacts, which is a multi-step sequence of analysis and calculations and team discussion, up to the identification of recommendations.

The goal of process risk management is to achieve control over the hazard factors existing in processes involving hazardous substances. Hence, the accepted indicators or categories of process risk are evaluated to determine risk acceptability. To this end risk acceptance criteria used as guidelines or recommendations in a given country. Since there are no established guidelines for risk acceptance criteria in Poland, hence each operator makes its own decisions on their application. The industry usually follows the semi-quality criteria by applying the risk matrix or uses the available risk criteria applied in other European countries or the USA with similar industrial plants.

If the designated level of risk is not accepted compared to the selected risk acceptance criteria, it is necessary to initiate the next stage of works by introducing proposals for additional safeguards and protection measures to achieve, at least, an acceptable level of risk. Obtaining an acceptable level of risk is one of the final stages of the works, which depends on the earlier processes and forms the basis for the submission of relevant information and proposals to the authorities of the CI operator as well as the owners and managers of risk and security of individual plants, systems or equipment in terms of proposed strategic decisions on organizational, technical changes or necessary financial expenditures.

2.6.7.3. *Explosion risk*

The explosion risk is a component of occupational, labor, facility as well as technology and process risks, which most often affect the following sectors in particular:

1) chemical and petrochemical industry,
2) mining industry,
3) food industry,
4) pharmaceutical industry,
5) timber industry,
6) raw material storage facilities and depots,
7) power sector,
8) transportation.

When launching the explosion risk assessment, all flammable substances present should be identified in the process of analyzing sources and threat factors. Determining the properties of flammable substances and their explosion parameters forms the basis for starting works on explosion risk assessment and is essential in the subsequent stages of conducting it. Relevant explosion parameters may include, in particular:

1. minimum ignition energy,
2. maximum explosion pressure,
3. explosion factors for dust and liquid gases and vapors,
4. flash point for the dust cloud and for a layer,
5. auto-ignition temperature for gases and liquid vapors,
6. flash point for the liquid.

The above parameters are the starting point for estimating the risk and potential effects of an explosion, indicating preventive measures, selecting equipment for operation in a given explosion-hazard zone, and designing a system to minimize the effects of an explosion. When assessing the risk of explosion, the CI operator's approach to dust explosiveness is important. The explosive properties of dust vary and depend on their granularity and moisture content, which generates two main types of consequences:

1) the data obtained from our own bases and the literature allow only to determine the preliminary risk, while the determination of the explosion parameters of dust samples is possible only under laboratory conditions;
2) the characteristics of dust are that a sample taken from one part of a process system may not have explosive properties, while from another part of the same system, it may acquire them, for example, as a result of drying or grinding.

The next step is to perform an explosion risk assessment and, based on this, develop an explosion protection document (EPD). The explosion risk assessment serves to indicate the spaces in which explosive atmospheres may exist or appear, because on the basis of them the CI operator, as the employer, is obliged to divide potentially explosive atmospheres into zones, classifying them on the basis of the probability and duration of the occurrence of explosive atmospheres.

An explosion risk assessment should be performed for:

- normal operating conditions, including maintenance,
- commissioning and decommissioning of facilities, systems and equipment,
- malfunctions, anticipated accidents,
- misuse that can be reasonably foreseen.

The Explosion Protection Document (ESD) is the complete and most important document (according to the ATEX Users Directive) that, pursuant to the regulations, should be owned by any entity where there is a threat of uncontrolled explosion, caused by the presence of flammable and explosive dusts, powders, vapors, flammable liquids, gases, mists and hybrid mixtures.

2.6.8. Key recommendations for ensuring technical security:

1. Threat analysis and risk assessment are carried out in the process of design, construction, commissioning of a facility, system or equipment for use, and in the process of its operation, repair and servicing.

2. Human errors are the most common causes of infrastructure operation disturbances.
3. Unnecessary overhauls can be detrimental, as in an effort to restore the equipment to an ideal state, there can be a so-called "novelty effect," which means that many components fail early in the early stages of operation.
4. In order to prevent potential accidents and ensure the long-term operation of a given CI facility, it is advisable to successively conduct a comprehensive assessment of technical condition based on security analyses and individually dedicated testing and measurement programs.
5. For structures where critical infrastructure components are located, the highest requirements for reliability of power supply and access to utilities should be adopted.
6. Achieving or maintaining an acceptable level of technical security is increasingly desirable not only because of legislation, but because of the growing importance of risk management processes and security culture. For many organizations, raising the level of technical security translates into competitiveness in achieving business and public missions.
7. Many CI operators, in an effort to strengthen their resilience, including in terms of technical safeguards[29], are implementing innovative technical and organizational solutions, applying higher technical security requirements and standards than indicated by national or international regulations. The level of technical security is also affected by proven and implemented Polish and foreign best practices resulting from the knowledge and experience of engineers, industries, and corporations or recommendations of independent interdisciplinary teams, e.g. in the field of risk management, anti-terrorist activities, anti-drone systems, cybersecurity and technology-process safety, energy, construction, hydrotechnical, fire protection, environmental protection or occupational safety, which, when implemented, constitute standards of expected requirements in a given field or area of security.
8. It is a good practice that the team carrying out the process risk assessment has its own leader and owner (manager) of the system, and has the structure and tools to work with, and has the appropriate number and type of experts who are aware of the work schedule consistent with the work plans of other teams performing risk assessments in the areas of CI security and organizational operations.

[29] Safeguards are the activities, systems, dedicated resources, and sets of prepared recommendations, policies, procedures, and instructions used in response to an identified threat in order to eliminate the threat and/or reduce the impact when it materializes.

2.7. Ensuring personal security

Ensuring personal security is a set of undertakings and procedures aimed at minimizing the risks associated with individuals who, through authorized access to critical infrastructure facilities, equipment, systems and services, may cause disruptions in its operation.

Members of the staff associated with critical infrastructure facilities, equipment, systems and services, as well as persons temporarily staying within the area of the CI (service providers, suppliers, visitors), may pose a potential threat to its operation. The position occupied in the structure of the CI operator determines the level of physical access to subsequent security zones and access to sensitive, not necessarily classified, information. Both of these privileges can be illegally used and serve to disrupt or jeopardize the operation of the CI (this includes service providers, suppliers and visitors).

More than 85% of frauds in companies is caused by people from within the company[30].

It is important to remember that many aspects of ensuring personal security are inextricably linked to other components of the CI security system, such as ensuring physical or ICT security. Only the complementarity of all components will provide a satisfactory level of assurance of CI security, protecting it against internal threats, such as disillusioned employees, provocations, competition or organized crime.

In order to systematize the information, the text has been divided into chapters corresponding to the next stages of actions with regard to people who may have a negative impact on the CI operation.

[30] Ernst & Young 9th International Fraud Survey – 9th Economic Fraud Survey – Fraud Risk in Emerging Markets.

2.7.1. Actions to be taken during hiring process

The basis for the effectiveness of ensuring personal security is to collect as much information as possible, which can be collected under applicable law, about a potential employee already in the recruitment process. In order to optimize the time, forces and resources used in the recruitment process, first of all, it is necessary to accurately profile the candidate, and a precise definition of the scope of responsibilities will allow you to determine the level of access to areas, rooms, depositories, etc., that will be granted to them and what sensitive information they will have.

It is advisable to carry out an assessment of the risk of CI operation disturbances associated with illegal use of information or access rights for various positions in the organization's structure. This assessment will form the basis for deciding on the depth of screening in the hiring process. It will also allow to better define the criteria that the candidate should meet. Such an assessment can be introduced and communicated in the form of a coordinated hiring policy in the organization.

2.7.2. Establishing identity

A prerequisite for further processing is verification of the candidate's identity. Do not proceed further if there are any objections to its correctness!

A person's identity consists of attributes assigned at birth (name, surname, date and place of birth, parents' names), individual biometric traits (biometrics of fingerprint, iris, palm, face, DNA) and components of biography (education, employment background).

The identity verification should be carried out primarily on the basis of original documents presented, including the names, surname, date of birth, address, holder's signature and photograph. It is necessary to check that the document being shown is issued by a competent authority and has a valid expiration date. It is mandatory to require documents that are difficult to forge, such as a passport, ID card or driver's license. It is necessary to verify the authenticity of the documents presented by the candidate. Employees performing such verification must have the appropriate knowledge and skills to perform such checks.

2.7.2.1. *Qualifications*

The verification of a candidate's qualifications should be based on verification of information contained in recruitment documents (resumes, forms, employment certificates, etc.). This will allow to assess the credibility and honesty of the candidate and get the information they would like to hide. As with establishing identity, all documents should be original. The authenticity of the submitted documents should be verified during the candidate's personal appearance during the recruitment process after the pre-selection stage.

- **Education**
  It is necessary to compare whether the information described in the resume matches the diplomas, certificates, etc. presented. Attention should be paid to the name of the school, university, company. Currently, many providers of courses or training use names similar to leading and recognized universities to attract participants in this way, without guaranteeing a high level of education. In addition, it is necessary to confirm dates and exact names of the courses and titles received. It is good practice to require a detailed plan for such courses or studies, and if in doubt, contact the university.
- **Experience**

  A similar procedure should be followed when checking professional experience. Require an employment background from at least 3 years (unless a different period is required by applicable regulations). Verify the length of employment, position and duties performed. Learning the reason for leaving will also be valuable information. Contacting previous employers is valuable because, in addition to receiving the information described above, it will also be possible to determine other skills of the employee, such as team work or diligent performance of duties. Therefore, it is also worth considering asking for references from your immediate supervisor.

- **Aptitude**

  Using a research tool, such as psychological tests (for positions for which it is reasonable to use such tests) and psychometric tools, it is possible to assess a candidate's personality, analytical abilities – aptitude for a specific job. In addition, the candidate may be presented with a theoretical problem from the scope of their potential duties and asked to solve it. This will allow to learn to some extent how their work and their ability to create cause-and-effect relationships.

2.7.2.2. *Criminal record*

When recruiting for key positions, which involve access to classified information, a screening process is carried out by the relevant state security services. However, the internal vetting process of the candidate should not be neglected. This is facilitated by the existing legislation included in the Emergency Management Law, among others, which allows to require an employee (or job candidate), to submit criminal record information, including information on whether their personal data is collected in the National Criminal Register.

2.7.3. Treatment of the employed

The priority in ensuring personal security is to thoroughly vet an employee (e.g., analyze submitted documents and verify their authenticity) even before hiring them, but security rules must not be neglected for those already employed in the organization. During the course of employment, in the event of a change of job position, the powers granted to the person should be reviewed and adjusted to the current job position. Any powers that the employee had in connection with their previous job position should be revoked. Crucial in this case is **information from the human resources department about the job position change** to other organizational units, including those responsible for security. It is also advisable to periodically review whether the powers granted to all persons – employees and third-party subcontractors – are indispensable.

2.7.3.1. *Non-standard behavior*

Observing employee behavior is one way to detect a potential insider threat. It should be emphasized; however, that this is not a matter of prying or surveillance, but only an assessment of the possibility of such a threat.

The team should be sensitized to changes in behavior and inform about those that may indicate a loosening of the relationship between the employee and the organization or their personal problems, such as:

- alcohol abuse;
- expressing views that approve of the actions of extremist groups;
- change of religion, political affiliation, social affiliation;
- inexplicable changes in personal life;
- lack of interest in the work being done, disappointment;
- symptoms of severe stress: aggression, choleric behavior;
- changing working hours, habits;
- non-standard interest in security systems;

- failure to follow safety procedures;
- unexcused absences.

The above list of non-standard behavior is not complete and cannot be the only criteria for disciplinary action. On the other hand, it can, along with other grounds, form the basis for assisting a person or controlling their activities in the organization. In particular, the occurrence of a whole range of premises must arouse the interest of those responsible for security in the organization.

2.7.3.2. *Access*[31]

One of the primary methods for ensuring the personal security of the CI is to restrict the access of the organization's employees to sensitive locations or resources located on the organization's premises as well as on ICT networks. Access should be granted only to the extent and at the time needed to perform tasks related to the job. Any attempt to reach restricted areas, networks or resources may indicate a potential threat from an employee.

Those in charge of security at set intervals should:

- verify access rights and restrict them if necessary;
- control, analyze and report all attempts at unauthorized access to places (premises) and ICT networks and resources.

Employees of the organization should be sensitized to attempts by any person to gain unauthorized access to restricted areas, and inform responsible persons of any such attempts that are noticed.

2.7.3.3. *Visual identification*

A visual identification of the employees of the organization as well as subcontractors and visitors is the easiest way to identify organizational affiliations and potential entitlements.

Every person in a CI facility should wear an ID badge with a photograph of the holder's face in a visible place. However, the ID should not contain (for security reasons, e.g., when lost) information about the access rights assigned. Instead, it should be marked with the appropriate color for the zone (building), in order to quickly identify any illegal employee in the area and take appropriate measures. Where justified, additional business clothing or other means of identification through clothing items (colored vests, helmets, etc.) should be introduced. When introducing a dress code, it is important to remember that it cannot be the only way of visual identification that allows access to the facility (the person

[31] For principles and methods for granting and controlling access see also chapters 2.5.1 and 2.5.3.

wearing a uniform with the company logo may not necessarily be the one they claim to be).

Do not wear badges in visible places outside CI facilities. This will make it difficult for unauthorized people to know the graphic design of the badges. People outside the organization should also not be allowed to take IDs outside the facility.

2.7.4. Protection of key personnel

In every organization there are individuals who have sensitive (unique) knowledge of how it operates, as well as experience and "institutional memory". They are particularly valuable to the organization, and at the same time potentially pose the greatest threat in case they act against the organization. In order to protect information of significant importance to the employer, separate non-compete agreements are concluded with them during and after the termination of the employment relationship. Such people should be provided with satisfactory working conditions by the employer, including salary, working hours and prestige. The employer should also provide opportunities for successive competence improvement and support from external entities. Protecting key personnel also means more stringent control requirements for them. Steps should also be taken to provide a replacement with similar qualifications and credentials.

2.7.5. Service providers / subcontractors

Employees of the entities, performing work on behalf of the CI operator, should be verified in a similar manner as in the case of recruitment, and in addition, it should be

checked whether the subcontractor in question is a member of a recognized and regarded association, has appropriate licenses, meets quality standards, has financial stability, etc.

Personnel recommendations, references from operators of the same system and examples of work already done are valuable, but even when they are very good, it is important to let the subcontractor know that they are being vetted.

Once the scope of the service has been established and the risk of disruption to the CI has been assessed, the level of access should be set, training should be provided to inform people of the threats involved and the procedures in place, and only then should any passes be issued or network access rights established. Any work that may adversely affect the CI must be carried out under the supervision of permanent CI staff.

2.7.6. Dealing with departing employees

Each of the employees leaving the organization is in possession of more or less sensitive information that can be used to the detriment of the organization. Therefore, in each case an assessment of the risks associated with the possibility of disclosure is necessary.

The estimation should be based on several guidelines. The first one is the employee's job position, which implies the level of access to information. The second one is the reason for leaving the workplace (voluntary, disciplinary, downsizing, contract expiration). The consequent steps include checking the employee's immediate plans, for example, whether the new place of employment will be a competing company.

The procedure during the notice period will be based on the risk assessment and primarily focus on restricting access depending on the level of risk. If the termination is immediate, full access shall be revoked, and the entire offboarding process shall be carried out under supervision. However, this does not mean that an employee leaving voluntarily should be given full access during the notice period. Decisions in this regard are made by the employer in specific situations. It is possible to relieve an employee from the obligation to perform work during the notice period.

An employee leaving the work position should return:

- company clothing, including uniforms (if any),
- badges, passes,
- company cell phones,
- business credit cards,
- business cards,
- room keys,
- one-time code generators,
- documents belonging to the organization,
- portable data drives, computers.

At the same time, persons in charge of granting access (physical and to ICT systems) should:

- block access privileges to systems, including deactivation of IDs, access cards, passwords,
- change access codes for doors, depositories,
- cancel credit cards,
- provide security personnel in advance with sufficient notice of the revocation of the employee's rights.

In the event of an employee's death, similar steps shall be followed. It is worth verifying whether current contact information for the employee's family is available, so that the aforementioned items can be immediately recovered.

It is necessary to consider changing access privileges (passwords, identifiers, cards) to resources, data, and areas (zones) that the departing employee shared with others as part of team work.

To raise CI operators' awareness of insider threats, it is worth creating a database of information on insider threats and incidents involving employees, subcontractors or visitors at the CI (sector) system level, as well as a mechanism for the secure exchange of this information. A centrally maintained database could include information collected from the sectoral level. Anonymous examples can help conducting a more thorough risk assessment and implement more effective protection measures.

A key factor for an effective personal security process is the prevention of abuse. The operator's actions such as promoting professional ethics, a policy of integrity in all company activities, ethical leadership, and effective control mechanisms effectively reduce the risk of intentional misconduct by employees.

2.7.7. Key recommendations for ensuring personal security:

1. Assess the risk of CI disruption for particular positions in the organization's structure.
2. Take plenty of time to check the credibility and competence of a new employee.
3. Raise awareness within the organization that any employee can pose a potential threat.
4. Identify and create the right conditions for key personnel.
5. Inform (human resources department) other organizational units, including those responsible for security, about the change of positions by employees.
6. Don't delay revoking access rights for employees who leave the organization.

2.8. Ensuring ICT security

Ensuring the ICT security of critical infrastructure means a set of organizational and technical measures aimed at minimizing the risk of disrupting CI operations as a result of unauthorized interference with control apparatus and ICT systems and networks, including acts of cybercrime and cyberterrorism in the broadest sense, as well as accidental (unintentional) actions by users.

Nowadays, a successful cyber attack on CI can directly affect the security of the state and its citizens. Critical infrastructure is vulnerable to cyber attacks carried out by both novice[32] and highly skilled cybercriminals, who can disrupt its operations, as well as to the consequences of random events such as system failures, malfunctioning equipment, or software issues managing the infrastructure.

2.8.1. Security of data processing

2.8.1.1. *On-premises solutions*

On-premises environments refer to data processing that takes place in physical or virtual environments, in owned or rented server rooms, which does not use public cloud solutions. The on-premises model is also undergoing a transformation and also refers to such a processing model, where server rooms or physical server services themselves are rented from other entities for selected types of processing.

Often the on-premises model for processing uses specific hardware or dedicated solutions (hardware combined with selected software and peripherals), e.g. provided only by a narrow group of providers and with a very specific purpose, for very specialized solutions (e.g. industrial or manufacturing process control).

In on-premises environments, there is currently a big trend toward automation and standardization of environments and the introduction of certain processes previously seen only in public cloud environments like Infrastructure as Code (IaC) management or environment cost allocation. The implementation of these processes, however, is fragmented and superficial due to the high heterogeneity of architecture, the range of physical and technical solutions used, as well as the high implementation costs associated, for example, with access to expertise in the market.

Independent of market changes, it is assumed that all the described processing models, including the on-premises model, will remain on the market in the long term, while there will be changes in the share of each

[32] Unfortunately, a great deal of technical knowledge is often not required to carry out a cyber attack. Some attacks can be carried out using off-the-shelf software, and the role of the attacker is reduced to choosing the method of attack and the target. Attackers using this approach are called *script kiddies*.

model and the further progressive standardization and automation of on-premises environments.

2.8.1.2. *Solutions using cloud computing*

Cloud computing

Over the past decade, the cloud computing model has become more widely used, both for IT solutions and increasingly for industrial automation solutions, and the so-called Internet of Things. Its use has also been considered for solutions requiring specific security measures, such as critical services or the processing of special categories of personal data.

The definition of cloud computing proposed in 2011 by NIST[33] is widely used, both in EU[34] and Polish[35] documents.

cloud computing – a pool of shared, accessible "on-demand" via ICT networks, configurable computing resources (e.g., networks, servers, storage, applications, services) that can be dynamically provisioned or released with minimal management effort and minimal participation by their provider.

It is worth noting the special characteristics of cloud computing:

- preconfigured and standard computing resources visible to the administrator as a separate product,
- independent, remote management of cloud resources by an administrator, including deployment or release of resources, without interaction with the cloud provider,
- standard service contracts and cost models.

The above characteristics of cloud computing bring it closer to standard (so-called "off-the-shelf") software, which is configurable but not modified by the user, and distinguish it from outsourcing, in which all components of the contract and ICT solution can be individually negotiated and modified, and modifications are introduced by the outsourcing company.

The key features encouraging the use of cloud computing include **scalability**, allowing for the deployment of extensive IT resources as well as their release when no longer

33 NIST 800-145, https://www.nist.gov/publications/nist-definition-cloud-computing

34 Examples: European Commission Cloud Strategy of May 16, 2019; European Banking Authority "EBA Guidelines on outsourcing arrangements" of February 25, 2019; 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 of network and information systems across the Union (the so-called NIS Directive).

35 Examples: Resolution No. 97 of the Council of Ministers of September 11, 2019 on the "Common State IT Infrastructure" Initiative; Communication of the Office of the Financial Supervisory Commission on information processing by supervised entities using public or hybrid cloud computing services of January 23, 2020.

needed, along with the **speed and ease of implementation**, a financial model based on operational costs rather than investments. Recently, **cybersecurity** can clearly be seen as one of the reasons for migrating to the cloud, as providers tend to have significantly greater resources and capabilities to implement cybersecurity measures. Cloud computing also provides the ability to easily achieve high resilience and the ability to maintain **continuity of operations**. The following part of this chapter outlines principles that should serve as guidelines when choosing cloud-based solutions.

The above description applies to public cloud computing, but it is also relevant in the case of implementing a private cloud model, such as within a group of entities, or a hybrid cloud that combines public and private cloud systems.

2.8.1.3. *Hybrid solutions*

Hybrid solutions have emerged with CI institutions using both on-premises (in various forms) and cloud environments. Simplifying, any data processing that occurs within a single enterprise, both in cloud computing environments and on-premises environments, can be referred to as a hybrid solution.

For example, internal, domain-specific systems are delivered in an on-premises model, while third-party collaboration solutions or universal services, such as email, data sharing and collaboration portals, are delivered in a service model ("software as a service"). A model of processing has also developed, in which a single information system includes certain resources in a public cloud environment (e.g., transactional systems), while additional functionalities (e.g., data analysis, data warehouses, reporting, security monitoring) are handled in a public cloud model. There are more solutions of this type, and recently there can be seen an increase in such projects in the areas of data analysis, also using artificial intelligence, IoT/OT event collection, security or data protection through additional backups in cloud environments. Wherever expansion of an IT system can be implemented by using a component, service or system available in public cloud environments, it can be called a "hybrid solution".

Hybrid solutions also influence the sharing and modification of the most common components of the IT environment, such as:

1) User identity.
2) Network.
3) Monitoring systems.
4) Safety systems.
5) Backup systems.
6) Collaboration and data exchange systems.

There may, of course, be more such components, but the ones listed are very common in implemented projects.

Additionally, the issue of hybrid computing will gain popularity not only because of the use of public cloud solutions, but also because of the use of third-party solutions (hosting, server space rental, service rental). Hybrid solutions will become the standard for data processing and will affect ICT security model of CI.

The use of cloud computing also requires the CI operator to assess risks other than those known from on-premises solutions, particularly when using a public cloud. Risk is primarily associated with the use of a subcontractor, over which the CI operator has limited influence in terms of its organization, changes, technical infrastructure, and personnel. It is particularly important to emphasize the need for simultaneous and joint evaluation of legal, contractual, organizational and technical conditions. The basic list of issues subject to risk assessment can be found in chapter 2.8.3.2

2.8.2. *ICT security principles for CI*

2.8.2.1. *Confidentiality, availability and integrity of information*

There are many models for identifying the characteristics of a properly protected ICT system. One of the more well-known and frequently used systems is the one that highlights the three most important characteristics of information security[36]:

- confidentiality,
- integrity,
- availability.

They mean that in order for a system to be considered as adequately secured, one must ensure that the information processed in this system is treated confidentially, in accordance with the granted access rights, it should maintain integrity so that it can be considered trustworthy, and there should be no problems with access to information for individuals with appropriate rights[37].

The above characteristics apply to software, hardware, and communication processes between the two.

Particular threats to a security model within this understanding are:

[36] In English terminology, the system is referred to as CIA (*Confidentiality, Integrity, Availability*).

[37] The above principles have been taken into account in the Regulation of the Council of Ministers ~~of April 12, 2012~~ on the National Interoperability Framework, minimum requirements for public records and exchange of information in electronic form and minimum requirements for ICT systems.

- unauthorized access to information and processes as a violation of their **confidentiality**,
- change or other disruption of information and executed processes as a violation of their **integrity**,
- blocking of access to information and processes as a violation of their **accessibility**.

The rapid development of ICT technologies, the focus on cost reduction, and the availability of a wide range of standard cloud computing products and services lead to their implementation in CI systems. This means that vulnerabilities of such products also become relevant to CI operators. Therefore, it is necessary to take appropriate organizational steps to ensure the proper selection of such products and services, as well as to manage vulnerability remediation, including updates.

2.8.2.2. *Organizational, technological, contractual solutions, and human resources*

The security of ICT systems requires ensuring security at the organizational level, in the technical (logical) sphere, as well as in the area of human resources.

Organizational solutions traditionally include security measures such as supervision over information technology in the organization with a hierarchy of goals, reporting on the results of implemented processes, the implementation of procedures, and the creation of a catalog of IT and cybersecurity activities within the organization. Organizational solutions take the form of policies, procedures, assessments, training programs aimed at employees, and audits or compliance reports.

The most important tool in the catalog of organizational solutions is the Information Security Policy. The information security policy allows for the effective and comprehensive management of the security of the data that is collected in the organization, especially in its information systems. An information security policy should include written goals, strategies and actions that clearly and structurally outline how to manage, protect, and disseminate collected data. The document should facilitate a thorough understanding of the purpose of safety procedures and is designed to raise awareness among the organization's employees of security threats and the risks involved.

A component of information security is asset management. The goal of the activities to be carried out should be the identification of assets, the determination of responsibility for their protection according to their importance, and preventing unauthorized disclosure and modification. An important factor in risk management is the frequency of its estimation and monitoring.

The final component of organizational safeguards is risk management. The implementation of this function may be dictated by the organization's mission, its business functions or the ability to use risk monitoring results to gain greater situational awareness. An increased level of this awareness, regarding the security status of the organization's information systems and the environments in which they operate, helps organizations better perceive and understand the risk of removal or destruction of informational assets.

Technical solutions include all cases of the application of equipment, software, and specific technologies within the context of the specificities of the information systems of Critical Infrastructure entities, which can perform operational, business, safety, physical protection, and crisis response functions. A key component in the technology area is software security, defined as the prevention of errors that could allow unauthorized control over an application, equipment, or system. Another example is the transmission system's immunity to interference, which is the protection of data transmission from interception or distortion of information. Another type of protection is to introduce monitoring of which employee has access to which categories of information. With this solution, in the event of a data leak, the organization can determine who is responsible for the leak and estimate the scale of the incident.

Examples of technical safeguards include the following:

1) **IPS – Intrusion Prevention System**

Intrusion Prevention Systems (IPS) is a type of network equipment that detects and blocks attacks on information systems. The equipment operates by monitoring key components of the system for unwanted behavior and events such as Internet worms, trojans, spyware or malware, and preventing them. An IPS can disconnect a computer network or interrupt a user session by blocking a specific IP number from accessing a resource or service, while some solutions also enable reconfiguration of the firewall or router.

2) **NGFW – Next Generation Firewall**

A "firewall" is a hardware and software solution that includes routers, servers, and software, restricting the flow of data packets between segments of a computer network in accordance with a defined security policy. In the case of Next Generation Firewall, the traditional firewall technology is enhanced with additional network equipment capable of filtering data packets, including deep packet inspection (DPI) and intrusion prevention systems (IPS). The purpose of implementing NGFW class tools is to inspect data packet on a greater number of layers of the OSI[38]model.

3) **WAF – Web Application Firewall**

[38] A reference model describing the structure of communication in a computer network.

Application "firewall" technology is a technology that enables information flows between computer systems, but without the direct ability to exchange data packets. The technology mitigates the risks associated with exchanging data packets between internal systems and external applications hosted on the corporate network. An application "firewall" is a piece of equipment or software located on a "hardened" operating system, e.g. Windows or UNIX, operating at the application layer of the OSI model. WAF analyzes information flows based on proxy servers, handling client requests by forwarding requests to other servers with their own network address for each service (e.g. FTP, Telnet or http).

4) **DLP – Data Leak Prevention**

This type of software is used to protect data from leaks, which applies to both accidental leaks, resulting, for example, from the carelessness of employees, and intentional actions. Most DLP-class solutions make it easy to locate and catalog sensitive information, as well as monitor and control the flow of information through corporate networks and endpoint equipment. This includes so-called "crawlers"[39] that search through data sets, network equipment that monitor network traffic, including those that perform deep packet inspection (DPI), and equipment that monitor end-user activities on workstations. Particularly important for DLP-class solutions is conducting an information security assessment, determining the value of processed data, and establishing policies and operational rules for the software and hardware components of the DLP system.

5) **SIEM – Security Information and Event Management**

The SIEM system is software designed to aggregate and analyze a substantial volume of data and information from both endpoint equipment and network monitoring tools, such as firewalls and Intrusion Prevention Systems. SIEM systems automatically aggregate and correlate data and logs related to cybersecurity events, in conjunction with analysis of historical data. Event correlation means that the SIEM system enables the creation of a single event having the nature of a cybersecurity incident. Rule-based correlation identifies the pattern of cybersecurity events, while statistics-based correlation defines the level of threat to information assets. Information from the systems can be used by internal teams like CSIRT or Security Operations Centers (SOC).

6) **SOAR – Security Orchestration, Automation and Response**

SOAR is a new technology in IT security that is gaining increasing importance, and is of particular interest to organizations with their own Security Operations Center or actively using a SIEM-class system. SOAR is a new class of IT Sec systems designed to more effectively manage cybersecurity events occurring in organization's IT/OT

[39] Software that collects information about data structure, pages and content.

systems. Their functionality primarily revolves around three areas: automating incident response processes based on playbooks, automatically enriching cybersecurity events with additional information through various integrations, and structuring processes based on roles and tickets.[40]

7) EDR – Endpoint Detection and Response

An EDR is a type of IT tool that monitors the endpoint equipment used in an organization and its corporate network (e.g., cell phones, laptops, workstations, Internet of Things equipment) in order to prevent cybersecurity threats. EDR technology is used to identify suspicious behavior and advanced, persistent cybersecurity threats on endpoints in the IT environment and to alert administrators accordingly. This is done by collecting and aggregating data from endpoints and other sources. This data may or may not be enriched with additional analysis in the cloud. EDR solutions are primarily an alerting tool rather than a layer of protection, but functions can be combined depending on the supplier. Data can be stored in a centralized database or transferred to a SIEM tool.

8) XDR – Extended Detection and Response

Extended Detection and Response (XDR) capabilities are a Software-as-A-Service model tool that offers comprehensive, optimized security, integrating security products and data into simplified solutions. Unlike systems such as endpoint detection and response (EDR), the XDR system extends security by integrating protection with a wider range of products, including an organization's endpoints, servers, cloud applications, and email. This way, the XDR system combines prevention, detection, investigation, and response, providing visibility, analysis, correlated incident alerts, and automated responses to enhance data security and combat cybersecurity threats[41].

In addition, in the technology area of industrial sectors, factors such as resistance to operating conditions and environmental influences, as well as reliability of operation over the life cycle of the equipment, i.e., time to first failure, should be taken into account. The organization should strive for the unification and standardization of solution architectures, including through the modernization or implementation of new systems to replace older, existing ones. The desired solution is the gradual phasing out of information systems that, due to their age and long-term use, are not subject to updates, security patches, or those that are incompatible with other systems responsible for security, taking into account the potential benefits and losses arising from the planned modernization. Complementary security measures should also be applied to older systems, including additional physical security measures such as fire protection,

[40] https://mediarecovery.pl/soar-czyli-wyzszy-poziom-soc/

[41] https://www.microsoft.com/pl-pl/security/business/security-101/what-is-xdr

intrusion and burglary alarm systems, access control, perimeter protection, or by transferring access accountability.

Contractual solutions involve the use of third-party service providers, including public cloud providers, telecommunications services, including extended services (the so-called OTT) or IT services, both related to implementation and technical support. To achieve an adequate level of confidentiality, integrity, and availability, the organization should check the terms of service (for standardized services) or ensure appropriate provisions in agreements (for recipient-specific services). Ensuring certified compliance with standards can help in the evaluation.

Examples of such agreements can be the terms and conditions included in the so-called SLAs (Service Level Agreements), which specify, among others, the service availability, service response time or the scope of the provider's/service provider's liability. Another type relates to agreements defining the technical and organizational conditions for providing the service, e.g. the role of the provider in the process of personal data processing, the rules for using subproviders, the presence of a business continuity plan or the rules for managing the provider's personnel. The provider's policies for handling the organization's data will be important, including data ownership, standard encryption policies, data retention and erasure processes, and a description of the process for terminating the service provision. Among the standards for contracting side ISO 27001, ISO 22301 or ISO 9000 are worth mentioning.

If, in the organization's opinion, the standard terms of service delivered by providers are not sufficient, the first step should be to determine whether extended services are available from a particular provider in connection with organizational changes or the use of additional technical solutions. Examples include solutions to increase availability (e.g., redundancy of critical infrastructure components, availability of technical support specialists and possibility of increasing response levels), security (e.g., other encryption methods, extended monitoring, additional data management tools, security incident management tools, but also a requirement of security clearance for support engineers), business continuity, etc.

The organization should also employ **specialists qualified** in various areas of ICT and cybersecurity, for example, in the areas of ICT solution development planning, their implementation, operation or monitoring. However, the speed of technology changes and the emergence of new cyber threats make it necessary for IT and cybersecurity professionals to improve their competencies on a regular basis, and the organization should guarantee an appropriate development path for its employees, such as a training program. The training program should be appropriately tailored to the needs of the entity in question, as well as to the organization's maturity level and the number of ICT systems used.

Therefore, the organization should adapt the training program to specific positions, not only those strictly related to cybersecurity, because in addition to automation specialists or information system administrators, it is vital, for example, to properly develop the public procurement description in terms of maintaining security standards and compatibility of new equipment or software with already existing resources.

2.8.2.3. *Training and testing*

Testing the systems and components responsible for the provision of services and processes within an organization allows for ensuring that they meet the assumptions established by the organization and other specified requirements related to their cybersecurity.

One of the overarching goals of testing information systems and components is to detect related vulnerabilities so as to take appropriate remedial actions. Vulnerabilities can be identified during activities such as:

a) conducting security audits and tests, which consist of vulnerability tests, penetration tests, audits for compliance with security standards, audits verifying compliance with security requirements, business continuity plan implementation exercises, and *red teaming* exercises, i.e., controlled attacks on the proprietary organization,
b) review of the information security management system and review of business continuity plans,
c) threat modeling and risk analysis,
d) security event management and proactive monitoring of system security,
e) security incident management (vulnerability as the cause of a reported security incident),
f) a consequence of active seeking of information about *zero-day* vulnerabilities matching the organization's asset base.[42]

The vulnerability scans are run in an automated manner and they do not target dedicated or lesser-known proprietary systems or applications. The vulnerability scanner allows for obtaining information on vulnerabilities related to popular solutions, as it uses a database of already-known vulnerabilities.[43].

Two scan types should be distinguished:

[42] C. Banasiński, M. Rojszczak (ed.), *Cyberbezpieczeństwo* [Cybersecurity], 2020, p. 152
[43] *Ibidem*, p. 154.

a) authenticated – implemented with information regarding authentication, access, etc.,
b) unauthenticated – performed as if the tested infrastructure was sniffed from "outside"[44].

Penetration tests also form an important part of verifying the security of systems and components, being a controlled attempt to break their security features. The activities performed in relation simulate attacks by hackers or crackers and their goal is to expose a vulnerability in a given system that would make it possible to break security features, break into or take control of the system. Testing its resistance to attacks is a five-step process:

I. Obtaining information on the tested object or area,
II. Scanning – a point-by-point inspection of the object or area under test with an electronic equipment,
III. Enumeration – acquiring information about the systems on which the service is based. It involves establishing an active connection and sending a query about the resources of the system providing the information in question, bypassing verification of the auditor's right to receive such data,
IV. Exploration, acquisition, extraction, exerciseing and extraction of knowledge from databases. It involves checking the possibility of obtaining them without the appropriate rights,
V. Reporting the strengths and weaknesses of the system under test, along with an assessment of the criticality of the weaknesses.[45]

Three types of penetration tests performed can be distinguished:

a) Black-Box – represents an attempt to break security features without any knowledge of the system under test. The auditor has information only on the attack target trying to break security features, faithfully mimicking the hacker's actions,
b) Gray-Box – these are attempts to break security features with limited knowledge of the system under attack. The attacker uses techniques used by hackers, but also has additional knowledge to penetrate security features more thoroughly,
c) White-Box – the attacker has complete knowledge of the system being attacked and seeks to break the security features in place on that basis to gain as much information as possible about the tested system[46].

[44] *Ibidem*, p. 155
[45] *Ibidem*, p. 156.
[46] *Ibidem*, p. 157.

Such types of tests provide a great deal of valuable information regarding the security of the analyzed systems, such as:

- the potential set of possible attack vectors,
- identified high-risk vulnerabilities, arising from the combination and use of low-risk gaps in a specific order,
- identified gaps that may be difficult or impossible to detect with automated tools for network or application vulnerability scanning,
- the assessment of the scale of potential business and operational losses as a result of a successful attack,
- examined capabilities of network security systems to effectively detect and respond to attacks,
- arguments related to the need to invest in personnel and technology in the area of cybersecurity solutions.

When using cloud solutions it is essential to check whether the provider regularly conducts and publishes the results of security tests of the offered solutions or platform.

In the case of internal information system security risks occurring in the organization, where technical security features and testing tools cannot be applied, it is reasonable to prepare a program of training and awareness activities for employees and professionals.

The entity should ensure that all employees of its organization have a similar level of baseline knowledge of cybersecurity topics and should conduct periodic training for all employees to regularly build cybersecurity awareness within its organization. The organization should also identify different target groups for training – from basic system users to those directly involved in IT and OT network and system security. The training scope should be appropriately tailored depending on the competencies needed to perform the tasks related to the given job.

Employees who are required by their scope of responsibilities to have advanced cybersecurity knowledge should have access to recurrent training and appropriate development paths. To this end it is reasonable to develop an appropriate training program for cybersecurity specialists so that their level of knowledge is at a high level, which will guarantee better preparation for the occurrence of a potential cyber attack and appropriate response.

To maintain an adequate level of cybersecurity knowledge in the organization, it is recommended to conduct periodic training sessions to remind people of the most important cybersecurity issues. Since everyone learns best from their mistakes, it is also recommended to conduct practical training from time to time, by, for example, organizing internal unannounced exercises on catching phishing campaigns.

Organizations should actively participate in organized national cybersecurity exercises, as well as, to the extent possible, in those organized at the international level.

Practicing and perfecting procedures contributes to a more efficient response to an emerging threat. In addition it allows for sharing experiences and best practices with other entities, as well as testing abilities of the organization's personnel. Such exercises usually involve a number of entities from different sectors – power, finance, transport, digital service providers, etc. Moreover, during the exercises, there is an opportunity to test the contact path with a national-level CSIRT or sector-level CSIRT.

2.8.3. *ICT security process*

2.8.3.1. *Zero Trust strategy*

The IT environment, in both small and medium-sized organizations, is increasingly complex. A single organization may have multiple internal networks, services are often provided remotely from another location, and the remote work model has become widespread. When it is difficult to clearly define the outer boundaries of our IT environment, the traditional (the so-called perimeter) model of ensuring cybersecurity is no longer sufficient, as once the first barrier is broken, an intruder can use lateral movement techniques to move within the IT environment without much hindrance.

Protecting the IT environment, especially for CI operators, cannot therefore now be reduced to protecting the network edge or end equipment from unwanted external action. Technological reinforcement and the addition of subsequent technical solutions is insufficient. This must be accompanied by a change in security organization.

The answer to the complexity of today's IT environments is a new cybersecurity model known as "Zero Trust"[47]. It is a technology-agnostic American NIST (National Institute of Standards and Technology) standard. **As one of the National Cybersecurity Standards published by the Government Plenipotentiary for Cybersecurity[48] the "Zero Trust" model is recommended for CI operators in all systems.**

[47] NIST Special Publication 800–207 "Zero Trust Architecture". 2020. Full version: https://doi.org/10.6028/NIST.SP.800-207

[48] https://gov.pl/attachment/8659d8de-6a83-4860-bcd1-d0648fbe9ead

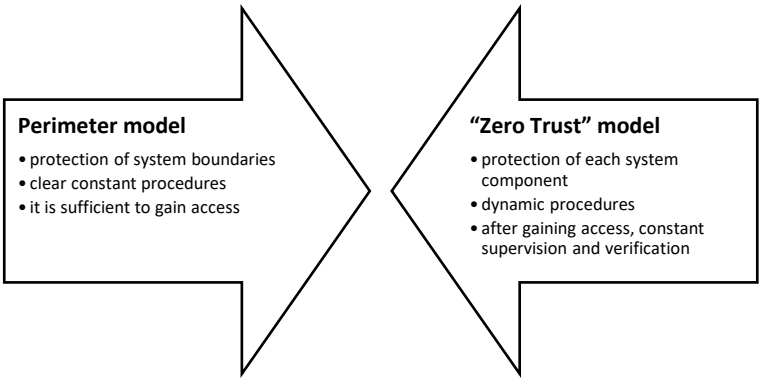


Figure 12Zero Trust model components.

The "Zero Trust" model is focused on protecting data and services, but should encompass all organization's resources (equipment, infrastructure components, applications, cloud and virtual resources) and entities (end users, applications and other components fed by data from resources).

"Zero Trust" means that it should be assumed in advance that the attacker is already present in the organization's environment, and the mere fact that the CI operator owns the environment does not mean a higher level of protection than in other environments. In such a situation **it is primarily recommended to conduct constant proprietary resource risk assessment, limit access to resources to minimum, and continuously monitor identity and security state of users** to whom resources are made available. Identity has recently become a key resource that should be subject to special protection.

All activities should be based on the following general assumptions:

1. **All data sources and computing services should be considered resources**, including private equipment (phones, tablets, watches) – if they have access to resources.
2. Regardless of the location in the network, **every communication must be secured**.
3. **Access to resources should be allocated on a separate session basis**. Subsequent resources should not be made available automatically.
4. **Access to resources should be determined by dynamic rules** defined also based on attributes other than identity (e.g., access to resources via cell phone is possible only if there is an up-to-date operating system, authorized for use, the user confirms identity and the session takes place during business hours).

5. There should be **continuous diagnosis and monitoring of all owned and related resources**.
6. **Authentication and authorization of resources should be done dynamically**, depending on the current level of trust/threat – using Identity, Credential and Access Management (ICAM) and resource management systems.
7. It is recommended to **collect as much information as possible about the current state of the IT environment** and use it on an ongoing basis to assess and improve the security state.

In general, it is necessary to ensure the continuous protection of the below-mentioned components of the IT environment, taking into account that the process of ensuring their security should include organizational and technical issues as well as human factors:

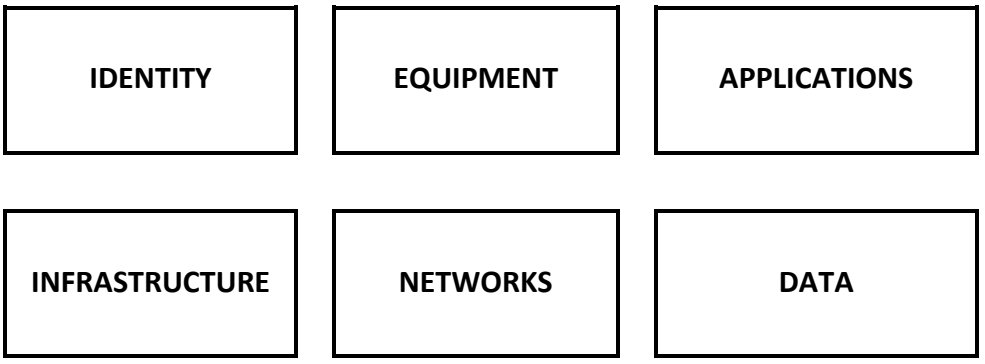


Figure 13 Basic components of the IT environment.

It should be noted that the principles stated above should apply both to the operator's own resources and to resources made available to the operator in the form of services, e.g. hosting, colocation, cloud computing. The remainder of this chapter includes the principles that allow CI operators to ensure security throughout the IT environment, in the areas indicated above.

However, it should be emphasized that the implementation of the "Zero Trust" model in organizations where solutions involving the protection of system boundaries are implemented should be done gradually, with a transition period in which traditional (perimeter) solutions will operate in parallel, and the environment and work rules will be gradually upgraded in accordance with the principles described above. This requires an organization to have a certain level of organizational maturity, consisting mainly of identifying and cataloging resources, entities, business processes, network flows, and dependency maps.

RECOMMENDATION: CI operators should strive for rapid, albeit gradual, implementation of "Zero Trust" principles through successive process changes and technological solutions to ensure the protection of the most valuable resources.

2.8.3.2. *Data processing models*

The use of cloud computing by Ci operators

New types of threats to the ICT environment, in particular state-sponsored attacks, as well as the experiences resulting from the war in Ukraine and legislative changes in several European countries (Estonia, Lithuania, Ukraine) allow us to conclude that the use of cloud computing by CI operators will help improve ICT security.

Thus CI operators should follow the following recommendations.

1. Cloud use is acceptable in the ICT environment of CI operators. This applies both to solutions directly related to CI and other solutions not directly related to CI.
2. Cloud computing feasibility should be assessed for each new ICT solution at the CI operator or when replacing an existing solution with a newer one or when implementing a newer version. **It is also recommended** that such an assessment be performed for the solutions used in terms of improving ICT security.
3. If the level of ICT security assurance in the public cloud is higher than for other solutions, then the CI operator should use the cloud solution, otherwise, a justification for another solution should be prepared.
4. The final decision on processing in the cloud should be made after conducting a risk assessment that takes into account the classification and evaluation of information processed in the cloud, ensuring an adequate level of data protection based on general and sectoral data protection regulations, and meeting the requirements of the relevant regulatory authority, if applicable to the CI operator.
5. **It is not recommended** for CI operators to use the public cloud if:
    a. The public cloud provider is a non-EU or non-NATO company, or is owned or controlled by non-EU or non-NATO entities. The law applicable to an agreement with a public cloud provider must be the law of Poland or another European Union member state.
    b. The data does not remain the exclusive property and under control of the CI operator.
    c. Data is not encrypted both at standby and during transmission.
    d. The provider does not provide a choice of data location (data processing center(s) also in the form of a so-called region). It is recommended that data should be located in Poland when data security and processing capabilities are identical to or better than those of location in EU or NATO countries.
    e. The provider for a particular cloud service does not have an information security management system developed in accordance with ISO 27001 along with a valid certificate issued by an accredited entity.
    g. The provider does not have a business continuity plan validated by a valid ISO 22301 certificate, the scope of which includes a specific service.

h. The provider does not ensure standard availability of the cloud solution of at least 99% in the agreement.
i. The provider does not indicate its responsibility in the agreement for its subproviders (subprocessors) and list of them is not available. It is recommended to cooperate with providers holding ISO 27036 certificate.
j. The provider does not ensure its responsibility in the agreement for its subproviders (subprocessors) and a list of them is not available.
k. The provider does not guarantee the security incident reporting process in the agreement.
l. The provider does not provide direct technical support in Poland.

6. When choosing cloud computing **it is recommended** that the CI operator should have additional options of:
   a. Choosing the length of the encryption key and the method for key selection and storage.
   b. Improving the availability of the ICT system in the cloud by using appropriate solutions.
   c. Using a dedicated cloud connection.
   d. Using technical support of individuals with security clearances.
   e. For the cloud services to be used by the CI operator, the provider has also provided valid and issued by accredited entities certificates for ISO 27017, ISO 27018, PN-EN 50600, SOC 1, SOC 2, NIST SP 800-53, NIST SP 800-207 standards or equivalent.
   f. In case the risk assessment indicates that audits by independent auditors are insufficient then audit at the provider is possible.
   g. The provider has been bound by the relevant code of conduct for selected services related to personal data processing.
7. **It is recommended** that the cloud administrator's tools should allow the implementation of security policies, in particular:
   a. Identity protection by implementing multi-factor authentication.
   b. Data classification.
   c. Protection against accidental or intentional information leakage by implementing DLP (Data Loss Prevention) tools.
8. If it is possible to use the Government Cloud Computing (GCC) it should be the first choice of the CI operator.
9. Regardless of the decision to use the public cloud, the CI operator should prepare **an evacuation plan** for ICT systems to the public cloud. In the case of using the public cloud, such a plan may be limited to preparing the process of moving the ICT system to another data processing center (or region) of the same provider, or the process of changing the provider.

2.8.3.3. *Threat types*

The chapter includes a sample list of vulnerabilities, divided into asset groups, with a corresponding list of potential threats that, if they occur, could affect the continuity of service provision.

Asset groups – physical locations (buildings)

Vulnerabilities:

- Failure of users to comply with the rules for the safe use of the building and rooms.
- Improper use of physical access control (ACS, physical protection).
- Location in a flood-prone area.
- Unstable electrical network.
- Inadequately protected switchgears.
- Negligence in terms of the inspection and maintenance of technical equipment (power supply, air conditioning, etc.).
- Inadequately performed repairs and maintenance.

Types of threats and security features:

- Physical damage
    a) Fire – fire detection system, extinguishing system, dry extinguishing system in the server room, duplicated computing center (server room), backup offices;
    b) Flooding – location of rooms reducing risk; duplicated computing center (server room), backup offices;
    c) Explosion – limitation of the amount of explosive substances, duplicated computing center (server room), backup office;
    d) Terrorist attack – access control, security services, video surveillance, duplicated computing center (server room), backup office;
    e) Strong radiation / electromagnetic pulse – to a limited extent duplicated computing center (server room), backup office;
- Natural phenomena
    a) Seismic phenomena – to a limited extent duplicated computing center (server room), backup office;
    b) Atmospheric phenomena – building structure and equipment, to a limited extent duplicated computing center (server room), backup office;
    c) Flood – structure, equipment and location of buildings, to a limited extent duplicated computing center (server room), backup office;
    d) Landslides – structure, equipment and location of buildings, to a limited extent duplicated computing center (server room), backup office;
- Technical failures

a) Loss or significant limitation of water supply – to a limited extent duplicated computing center (server room), backup office;
b) Loss of power supply – guaranteed power supply, power supply from two sources, power generator sets, duplicated computing center (server room), backup office;
c) Air conditioning system failure – equipment redundancy; duplicated computing center (server room), backup office;
d) Telecommunications equipment failure – redundancy of equipment and connections, duplicated computing center (server room), backup office.

- Unintentional harmful human actions
  a) Accidental cut-off of utilities (water, electricity, telecommunication connections) – redundancy of equipment and connections, duplicated computing center (server room), backup office.
- Intentional harmful human actions
  b) Equipment theft – access control, security services, video surveillance, duplicated computing center (server room), backup office;
  c) Acts of vandalism – building structure and equipment, access control, security services, video surveillance, duplicated computing center (server room), backup office;
  d) Enforcement – access control, security services, video surveillance;
  e) Strike of services responsible for the maintenance and operation of facilities – to a limited extent, duplicated computing center (server room), backup office.

Asset groups – technical and system infrastructure necessary for the operation of ICT systems and applications

Vulnerabilities:

- Sensitivity to environmental factors (moisture, too low humidity, dust, pollution, etc.),
- Sensitivity to electromagnetic radiation,
- Sensitivity to voltage and frequency fluctuations,
- Lack of or delayed periodic use of equipment,
- Improper handling of storage media,
- Lack of effective control of configuration changes,
- Lack of diligence in media destruction,
- Inadequate infrastructure management (unused and inadequately secured accounts, enabled unused services, unnecessarily open ports, etc.),
- Unprotected data cabling/connections (including telecommunications terminations),
- Inadequately protected sensitive traffic,
- Occurrence of a failure single point,
- Lack of or weak authentication (including weak privileged account passwords),
- Service overexposure,

- Inadequate rules for granting infrastructure management rights,
- Acting with excessive rights,
- Improperly secured network structure,
- Lack of separation between front-end and back-end servers (application – database),
- Inadequate network management,
- Unsecured connection to the public network,
- Unsecured or improperly secured Wi-Fi network,
- Possibility of plugging an unauthorized equipment into the LAN,
- Use of equipment of unknown origin,
- Lack of or insufficient mechanisms for monitoring infrastructure performance,
- Lack of or inadequate business continuity plans,
- Lack of or outdated or insufficient technical documentation.

Types of threats and security features:

- Physical damage
    a) Electrostatic discharge – reset, maintaining proper humidity (air conditioning with humidification option);
    b) Strong radiation / electromagnetic pulse – to a limited extent equipment redundancy, duplicated computing center (server room), backup office;
    c) Strong thermal radiation – to a limited extent equipment redundancy, duplicated computing center (server room), backup office;
    d) Physical damage (e.g., fall during maintenance activities, overhaul works, etc.) – OH&S rules, to a limited extent equipment redundancy, duplicated computing center (server room), backup office.
- Technical failures
    a) Total equipment failure – equipment redundancy, duplicated computing center (server room);
    b) Damage to a piece of equipment module/component (including storage medium) – equipment redundancy, disk arrays, backups, service agreements, duplicated computing center (server room), virtualization;
    c) Power supply outage – guaranteed power supply, emergency power supply, power generator set, duplicated computing center (server room),
    d) Software (firmware) bugs – service agreements, vulnerability management.
- Unintentional harmful human actions
    a) Configuration errors – configuration standards, change management, testing, training;
    b) Administrator mistakes – configuration standards, change management, testing, training;
    c) Organizational deficiencies – incorrectly defined or not defined responsibilities – procedures, policies and rules, auditing;

d) Accidental information leakage – encryption of media and mobile equipment, information classification, DLP systems, secure printing;
e) Insufficient technical documentation – solution selection process (documentation completeness assessment), testing, auditing;
f) Lack of manufacturer/provider support – service agreements, avoidance of unsupported technologies;
g) Insufficient administrator competencies – recruitment rules, training, documentation (instructions), configuration standards;
h) Inadequate network architecture – verification, security testing;
i) Use of equipment not adapted to the needs – business needs analysis, solution selection process, testing;
j) Insufficient infrastructure capacity – capacity management, virtualization;
k) Monitoring errors – definition of the scope and frequency of monitoring, monitoring and alerting systems;
l) Provision of the equipment management capability from an external network – policies and rules, network configuration, network security equipment;
m) Credential sharing – policies and rules, event logging, credential management mechanisms.

- Intentional harmful human actions
  a) Theft – access control, security services, video surveillance, duplicated computing center (server room), backup office;
  b) Sniffing including communication interception – network architecture, certified equipment, shielding, network and equipment configuration, network security systems, communication encryption;
  c) Malware operation – network security systems, antivirus and antimalware software, network architecture, minimum right principle;
  d) Software replacement / reconfiguration – network security systems, network architecture, change management, minimum right principle, central management systems, software installation, central system configuration management systems;
  e) Information falsification – event logging, backups, duplicated computing center (server room), minimum right principle;
  f) Abuse of access rights – procedures and policies, event logging, monitoring, management of privileged accounts,
  g) Rights escalation – minimum right principle, vulnerability management, regular updates and patches;
  h) Use of known vulnerability – vulnerability management, network security systems, network architecture, minimum right principle;
  i) Enforcement / sociotechnics – training, policies and rules, minimum right principle, network architecture, network security systems;
  j) Making the equipment unavailable (damage, shutdown, DDoS) – anti-DDoS systems at the level of the Internet connection operator, CDN operators, duplicated connections, duplicated computing center (server

room), network architecture, minimum privilege rule, access control system, security services;

k) Damage to cabling – duplicated connections, duplicated computing center (server room); network architecture, access control system, security services, video surveillance, infrastructure monitoring systems;

l) Use of publicly available information – information classification, procedures, policies and rules, network security systems;

m) Breaking through security features and acquiring information (equipment configuration, internal network structure, etc.) – network security systems, network architecture, minimum right principle, vulnerability management, security testing, access lists.

Asset groups – systems and applications

Vulnerabilities:

- Lack of or insufficient application testing
- Known and still existing vulnerabilities
- Failure to update systems and applications on an ongoing basis
- Maintaining an active session for longer than required
- Failure to log out from the operator or administration station
- Lack of or insufficient event logging
- Lack of or insufficient application and configuration integrity checks
- Inappropriate access rights
- Improper change management
- Inappropriate password policy
- Incorrect configuration
- Lack of or inadequate authentication mechanisms
- Unsecured or improperly secured data in databases (including credentials)
- Lack of or outdated or insufficient technical documentation
- Lack of or insufficient backups
- Running unnecessary services
- Presence of active unused accounts
- Lack of or insufficient control over the reconfiguration of systems and applications
- Lack of or insufficient control over access to data

Types of threats and security features:

- Failures:
  a) System/application failure – duplicated computing center (server room), application architecture (cluster/redundancy), backups, resource virtualization, application testing;
  b) Application malfunction as a result of an unidentified error – monitoring of application operation status, application testing, change management;

c) Unacceptable system/application response time (e.g., as a result of overloading) – monitoring of application operation status, capacity management, performance testing and application saturation;
d) Failure to make backup – reporting of a system intended to make backups, verification of backup making.

- Unintentional harmful human actions:
  a) Making system/application unavailable – duplicated computing center (server room), application architecture (cluster/redundancy), resource virtualization,
  b) User errors – application architecture and design(internal data validation, roles and rights system), training, user documentation, testing,
  c) Incorrect system/application configuration – application documentation, monitoring of application operation status, application test, change management, use of a separate development and test environment;
  d) Leaving identified vulnerabilities non-handled – vulnerability management, application documentation,
  e) Use of unverified system/application components – application architecture and design, application requirements, procedures, policies and rules, application testing, use of a separate development and test environment,
  f) Disclosure of authorization data to unauthorized persons – procedures, policies and rules, minimum right principle,
  g) Introduction of unverified modification leading to vulnerability – procedures, policies and rules, minimum right principle, change management, application testing, application documentation, use of a separate development and test environment,
  h) Accidental backup deletion – procedures, policies and rules, backup process automation, duplication of backups.

- Intentional harmful human actions
  a) Making system/application unavailable – duplicated computing center (server room), application architecture (cluster), resource virtualization, network security systems, policies, procedures and rules, event logging;
  b) Limiting system/application availability – duplicated computing center (server room), application architecture (cluster), resource virtualization, network security systems, policies procedures and rules, event logging;
  c) Deletion or unauthorized modification of data – backups, network security systems, network and application architecture, minimum right principle, policies, procedures and rules, event logging, access lists;
  d) Unauthorized data extraction – network security systems, network and application architecture, minimum right principle, policies, procedures and rules, event logging, access lists;
  e) Change of system/application configuration resulting in new vulnerabilities – network security systems, network and application architecture, minimum

right principle, policies, procedures and rules, event logging, vulnerability management, application testing, access lists;

f) Rights elevation and performance of harmful activities – network security systems, network and application architecture, minimum right principle, policies, procedures, and rules, event logging, vulnerability management, application testing, access lists;
g) Malware installation (at an administrator or operator station) – network security systems, network and application architecture, minimum right principle, monitoring, antimalware software, event logging, vulnerability management, access lists
h) Malware operation – network security systems, network and application architecture, minimum right principle, antimalware software, event logging, vulnerability management.

Asset groups – information resources, data, documents

Vulnerabilities:

- Failure of users to comply with information handling rules
- Inadequate protection of information from destruction or unauthorized access
- Lack of copies of information resources (paper)
- Failure to update documentation
- Incomplete or insufficient quality of information
- Inadequate data protection on storage media
- Lack of or inadequate process of backup making
- Inadequate data access rights
- Lack of authorization for information processing means

Types of threats and security features:

- Environmental risks:

a) Fire – fire detection system, extinguishing system (office), dry extinguishing system (server room); duplicated computing center (server room); backup office, security services, employee training;
b) Flooding – location of rooms reducing risk; duplicated computing center (server room), backup office.

- Technical failures

a) Storage media damage – storage media redundancy (RAID, arrays), backups;
b) Failure resulting in temporary unavailability of information resources – duplicated computing center (server room) (data replication).

- Unintentional harmful human actions
  a) Accidental destruction or deletion – backups, duplicated computing center (server room) (data replication);
  b) Accidental making available to unauthorized persons– procedures, policies, and rules;
  c) Loss – backups, data encryption, procedures, policies, and rules;
  d) Accidental modification (integrity violation) – backups, duplicated computing center (server room) (data replication), change management.

- Intentional harmful human actions
  a) Theft – backups, duplicated computing center (server room) (data replication), procedures, policies, and rules;
  b) Physical damage – backups, duplicated computing center (server room) (data replication), procedures, policies, and rules;
  c) Information (data) modification – backups, duplicated computing center (server room) (data replication), event logging, procedures, policies, and rules.

Asset groups – personnel

Vulnerabilities:

- Personnel absence
- Personnel shortages
- Personnel irresponsibility and carelessness
- Inadequate recruitment procedures
- Inadequate training
- Low security awareness
- Incorrect use of equipment and applications
- Lack of monitoring mechanisms
- Lack of or insufficient rules for the use of telecommunications equipment and resources
- Personnel vulnerability to bribery
- Failure to comply with physical protection rules

Types of threats and security features:

- External factors
  a) Illness or unavailability – substitutability
  b) Insufficient knowledge – training
  c) Personnel shortages – personnel policy, risk management
- Internal factors
  a) Lack of motivation – human resources policy
  b) Conflict of interest – procedures, policies, and rules

c) Sabotage – access control system, security services, video surveillance, right minimization principle, monitoring systems, event logging
d) Strike – risk management

Asset groups – services

Vulnerabilities:

- Lack of or inadequate provider selection procedures
- Lack of service support
- Lack of supervision over the implementation of external services (service technicians, software providers, cleaning service)
- Lack of or insufficient monitoring of external providers' activities
- Lack of or inadequate monitoring of the service provision quality
- Lack of or inadequate security clauses in service agreements
- Inadequate rights of third-party service providers
- Lack of adequate restrictions on physical access (including lack of supervision)
- Lack of emergency procedures for selecting alternative providers
- Insufficient access to spare parts

Types of threats and security features:

- Unintended harmful actions:
  a) Loss of executive capacity (e.g., termination of business, profile change, loss of key personnel) – cooperation with proven providers, security provisions in agreements, monitoring of the service provision quality, emergency procedures for selecting a new provider;
  b) Limited executive capacity (e.g., loss of part of personnel, loss of important competencies) – cooperation with proven providers, security provisions in agreements, monitoring of the service provision quality, emergency procedures for selecting a new provider;
  c) Inadequate quality of the service provided – cooperation with proven providers, security provisions in agreements, monitoring of the service provision quality, emergency procedures for selecting a new provider;
  d) Lack of documentation for the service provided – cooperation with proven providers, security provisions in agreements, monitoring of the service provision quality.
- Intentional harmful actions:
  a) Intentional modification of system operation parameters – cooperation with proven providers, right minimization, monitoring of provider work, testing;
  b) Intentional data modification – cooperation with proven providers, right minimization, monitoring of provider work, testing;
  c) Failure to comply with agreement performance terms and conditions – cooperation with proven providers, security provisions in agreements,

monitoring of the service provision quality, emergency procedures for selecting a new provider;

d) Introduction of undocumented functionality into the application – cooperation with proven providers, right minimization, monitoring of provider work, testing;
e) Information theft – cooperation with proven providers, right minimization, monitoring of provider work;
f) Equipment theft – cooperation with proven providers, access rights limitation, monitoring of provider work;
g) Sabotage – cooperation with proven providers, right minimization, access rights limitation, monitoring of provider work, testing.

2.8.3.4. *Shared responsibility for the process continuity*

Security&Compliance is a shared responsibility between the cloud computing service provider and the client. This shared responsibility model helps reduce the operational burden on the CI operator, as the cloud computing service provider operates, manages, and controls components from the host operating system and virtualization layer to the physical protection of the facilities where the service runs.

CI operators should carefully consider and understand the operation of the services they choose, as their responsibilities vary depending on the type of services they use, the integration of those services into their IT environment, and applicable laws and regulations. This is also a very important component when it comes to considering and planning for business continuity and processes that will be moved to cloud computing, as they are fundamentally different from the traditional on-premises model.

In simple terms, it is assumed that the cloud computing service provider is responsible for protecting the infrastructure on which these services run. This infrastructure consists of hardware, software, networks, and facilities that support cloud computing services.

The responsibility of a CI operator is determined by the type of cloud computing services it chooses. This choice has consequences and determines the amount of configuration work that the operator must do as part of his responsibilities in the security area. For example, a service classified as infrastructure as a service (IaaS) as such requires the client to perform all the necessary tasks related to security features configuration and management. CI operators who implement such a service are responsible for managing the host operating system (including updates and security patches), any applications or tools installed by the client on the instances, and firewall configuration. In the case of PaaS services, the cloud computing services provider handles the infrastructure layer, operating system, and platform, while the CI operator gains access to the endpoints for data storage and retrieval. Moreover, clients are responsible for managing their data

(including choosing encryption options), classifying their resources, and using tools to apply appropriate rights and manage access to them.

Such a shared responsibility model between cloud computing services and CI operator also extends to the area of compliance and control. Just as the responsibility for operating the IT environment is shared between the cloud computing service provider and its operators, management, operation, and compliance verification are also shared. A cloud computing provider can help ease the burden on the operator by managing controls related to the physical infrastructure deployed in its environment, which previously could have been managed and were the responsibility of the operator. Since each cloud computing service deployment is different, clients may delegate the management of certain aspects of compliance to the service provider, resulting in a (new) distributed control environment. CI operators can then use the control and compliance documentation available to them for a particular cloud computing provider to perform the required procedures/audits in their assessment and verification area.

The same perspective should be used to look at the continuity of the process we want to move to cloud computing. The process is also divided into a part that will be the responsibility of the cloud computing service provider and a part that will be the responsibility of the operator. This will also be a result of what kind of cloud computing services will be used to implement it. On the cloud computing provider side, it is worth noting that it is ISO 22301 certified – Business Continuity Management as well as ISO 27001 certified with Business Continuity Management (BCM), Business Impact Analysis (BIA), Business Continuity Plan (BCP) components. For more detailed information on what cloud computing service providers are doing to ensure business continuity, it's also worth looking at reports such as C5 (Cloud Computing Compliance Controls Catalogue) or the SOC (Service Organizations Control) 2 type 2 report.

It is recommended for CI operators to verify reports and certifications from the business continuity area by inspecting cloud computing service provider attestation reports. The following are examples of areas to pay attention to:

- Does the cloud computing service provider have a resiliency-type program that includes processes and procedures by which it identifies, responds to, and remediates a major event or incident;
- Are emergency plans and incident response manuals maintained and updated to reflect emerging business continuity risks and lessons learned from past incidents;
- Are the service team's response plans tested and updated during operations and is the cloud computing provider's resilience plan tested, reviewed and approved annually by senior management;

- Has the cloud provider established a CSIRT (Computer Security Incident Response Team) that contributes to the coordinated resolution of specific security incidents and are operators affected by security incidents informed in a timely and appropriate form.

It is also important to understand the level of availability not only at the level of the region/zone of availability of a given cloud computing service provider itself, but of individual services and their level of availability (SLA – Service Level Agreement is used for this). This information should be available as standard on the websites of cloud computing service providers.

In case of very critical overloads deploying infrastructure across multiple regions with data replication and continuous backups to minimize the impact on process continuity may be considered. It is vital to take into account how the cloud computing provider has designed the availability zones in the region and whether a significant distance is maintained between them and the location is carefully planned so that any disasters affect only one zone and not others.

2.8.4. *Building resilience*

Cyber security is often wrongly equated with the protection of endpoint devices by antivirus software. In fact, cyber security must be built in every area. According to the Zero Trust principle – an organization's resilience to ICT threats should include: identity, data, software, infrastructure, applications and networks. Identity protection should include strong user authentication, verification of the devices used by the user, verification of permissions (minimal, necessary, granted temporarily) and verification of ongoing activity (for anomalies, including, for example, data leaks or extraction).

In addition, in terms of white/black lists, in the era of dynamic domains and variable addressing, the proposed solution should be considered insufficient and needs to be expanded with refutation mechanisms based on the use of AI and cooperation between companies, providers or cyber security teams.

A special case is the protection of industrial automation, which will be described in Chapter 2.8.9.

2.8.4.1. *Endpoint devices*

The ubiquity of access to the Internet by the workstations of an organization's employees causes a significant increase in vulnerability to threats arising from it. Therefore, the recommended solution is to restrict the possibility of access from employee workstations, connected to the Internet, to systems that support CI. However, if necessary, to mitigate this vulnerability, the protection of workstations used by the

organization's employees, including those directly handling CI, should rely on three fundamental security pillars:

Software update

Note that in addition to the widespread awareness of the need to update operating system software, it is also necessary to update applications. Not all operating systems and applications have automatic update capabilities. If it is possible to automate the software in question (AV operating system), one of best practices is to run your own update center. This gives you control over the installation of updates and reduces the risk of installing updates that lead to software failures. In addition, due to the need to maintain the correct operation of applications (e.g., in the case of automation systems), it is often not possible to use this function, and the introduction of a change to the software involves a change management procedure and a series of tests to confirm that the update has no impact on the functioning of the system.

A part of the change management procedure for software upgrades should be a short risk analysis due to the emergence of a new threat. The common vulnerability scoring system [49](CVSS) standard can help with this. The use of a threat assessment of the system vulnerability to which the update is related, using this standard, allows for a standardized assessment that can guide the update decision. Sometimes this assessment is made by the manufacturers themselves[50]. However, if such an assessment is not available, it is possible for the user to carry it out independently, for example using the CVSS[51] calculator.

Attention should be paid to the process of managing applications at the workstation level by revoking permissions for software installation by the user or providing internal software stores that allow installation by the user, but only of approved and/or configured software. It is also recommended to implement a central system of application management or distribute configured applications where the user has limited ability to change settings.

Firewalling

The principles to be used in protecting workstations through the use of a firewall are not fundamentally different from those described earlier[52]. The main difference is that so-

[49] http://www.first.org/cvss/cvss-guide.html
[50] For example CISCO http://www.cisco.com/web/about/security/intelligence/Cisco_CVSS.html
[51] For example provided by NIST http://nvd.nist.gov/cvss.cfm?calculator
[52] See Chapter 2.8.3.4 Access control.

called personal firewalls are used as workstation protection. They are either built into the operating system or constitute a separate, dedicated software.

Protection against malware

Protection against malware complements software updates and firewalling. The term "malware" can be applied to any type of software that interferes with the operation of a computer without the owner's knowledge. Malware can be distinguished into:

- Ransomware,
- Computer viruses,
- Internet worms,
- Trojan horses,
- Spyware,
- Crimeware.

It can perform a wide variety of functions, from simply collecting information about a system user to carrying out criminal activities. In practice, it is difficult to distinguish between different types of malware, moreover, it is increasingly pointless to do so, as more and more often individual programs combine malicious functions.

Protection against malware is to install appropriate security software. The software mostly protects against known malware. However, note that the number of new types of malware (or at least slightly modified to improve its camouflage) is very high[53]. Therefore, in practice, it is not possible to effectively detect all existing viruses on the Internet. This, of course, does not change the need to use the appropriate software.

Keep in mind that antivirus software protects against known malware, and is largely based on virus signatures, although it also has built-in heuristic mechanisms or HIPS-type functionality. Also existing Endpoint Detection and Response (EDR) class solutions are worth considering, as they do not operate on signatures, but on endpoint events, so they can detect unknown threats.

2.8.4.2. *Data*

Access control

Access control to resources is a fundamental way to ensure ICT security. The main principle to be followed in setting rules for access to resources is the "need to know" principle. According to this principle, access rights to particular resources shall be granted only to those for whom this access is necessary.

[53] The Virus Total website analyzes tens of thousands of new malware files every week http://www.virustotal.com/stats.html

There are two methods for verifying access rights to an ICT system. The first involves a detailed reconsideration of access rights. It is worth considering in this analysis the frequency of access to date and the type of accessed data (whether it coincides with the actual needs of those with access rights). The advantage of this method is the systematic approach and full continuity of the task. The disadvantage is that it is likely that many attempts to restrict access will encounter serious resistance, related to more or less true justifications for the need for this access. Therefore, there is a second, more radical method. Access is denied to all users of the system (except perhaps those obvious cases of necessity of access, such as access for billing accountants to the system for entering settlements) and cases of attempted access to the system are observed. These cases alone demonstrate the potential need for access to information. They should then be further analyzed in detail and a final decision should be made on the access and its scope.

One of the biggest risks is granting access rights or changing the scope of access on a so-called "temporary basis". This is usually dictated by an actual momentary need, and often by the need for access from outside the company (which is normally prevented). Practice shows that often this temporary access lasts much longer. Therefore, it should be avoided in the first place, and in justified cases granted with a time limitation, controlled automatically by the system (provided it allows for it).

In addition to the "need to access information" principles described above, other, more technical, access control tools should be used:

Access control by ensuring proper network architecture

In particular, it is the use of Virtual Local Networks, which are logically separated computer networks within a larger physical network. With this separation, it is possible to separate network traffic, which is an important protection principle. Important additional elements of virtual network security include the use of MAC (Media Access Control) address-based traffic control and appropriate IP packet filtering policies[54].

It is good practice to apply network access control policies based on "computer health", i.e. whether it is equipped with the latest updates as intended by the system administrator. If the computer does not pass the verification properly, it is redirected to another subnet where the necessary software components are automatically updated.

Use of firewalling

Firewalling is one of the basic security techniques. It is implemented on the basis of appropriate software or a complete solution in the form of dedicated hardware and software. By using a firewall, it is possible to protect the traffic incoming to the

[54] For more on security rules for creating virtual networks, see the document "VLAN Security Guidelines" http://www.corecom.com/external/livesecurity/vlansec.htm

organization network and the traffic leaving the organization, each time pointing only to the one that is allowed. Another important feature implemented with a firewall is traffic monitoring and identification, and allowing authorized users into the network by setting up an encrypted connection, called a Virtual Private Network[55].

Access from outside

Access to the organization's resources from outside should be done in a secure manner, keeping in mind mainly encrypted access (the choice of protocols and encryption algorithms should be made based on their vulnerability to cryptanalytic attacks) and based on strong authentication. This creates a secure encrypted channel of communication with company resources. One of the best ways of strong authentication is to use multi-factor authentication (MFA), preferably in the form of hardware keys or application keys/tokens.

When organizing access from the outside, it is also worth covering access for software and hardware service companies with special communication security. This type of access is very often organized by external companies on their terms. Unfortunately, the priority with this access is to make it as easy as possible for service technicians, very often without paying close attention to safety rules.

Special attention should be paid to remote access (e.g., from service companies) to industrial automation system assets. This type of access should be granted only in justified cases, each time recorded and confirmed by the person responsible for the area/system. The remote access channel should be closed when the work is completed and reopened only when there is a legitimate need for its use. All work carried out using remote access should be recorded and monitored on an ongoing basis.

In Ci-handling networks, dial-up access is still a very popular way to access devices. Using this type of access is not the safest approach, and it is recommended to avoid it. However, there are methods to properly secure it if its use becomes necessary. When using dial-up access, care should be taken to ensure the implementation of the following security principles:

- control of login data,
- access control using a suitably strong password, possibly a one-time password,
- a system for detecting calls from unauthorized sources and alerting on them.

Blacklisting and whitelisting

One of the possible methods of access control is the creation of "black lists" and "white lists". These techniques are often used in anti-spam protection. Also, they can be used

[55] Firewall specific configurations vary by type and manufacturer. General rules for firewall configuration can be found at http://msdn.microsoft.com/en-us/library/ms898965.aspx

to protect against malware that installs itself without the user knowledge when visiting an infected website[56]. The idea behind the "black list" is to indicate those addresses (e-mail, IP, domain) that are not allowed in inbound traffic. All other addresses will be allowed. The "white list", on the other hand, contains those addresses that will be accepted as source addresses. No other addresses, that are not on the "white list", will be accepted. In addition to the aforementioned ability to use this technique in protecting Internet communications (spam, drive-by-download), it can also be successfully used in managing internal and external networks – in setting access rights to individual applications.

Proxy server

Another access control technique is the use of a proxy server. In addition to the security function, it can also perform the task of improving traffic efficiency, for example, by mediating access to Internet resources that, if they were previously downloaded by one user, are already made available for subsequent users from the proxy server, rather than from the original service, greatly speeding up data transmission. On the other hand, the basic security features for a proxy server are the ability to inspect traffic before it is delivered to the end user (this way, for example, antivirus inspection of websites can be performed) and the ability to hide (if necessary) selected IP addresses from the protected network

Encryption

Unauthorized access to data is often a result of physical theft or loss of a device or media on which the data was stored. As such, care should be taken to ensure that any sensitive data is recorded only in encrypted form. For mobile devices, such as laptops and smartphones, the most practical and secure solution is to use full disk encryption. In practice, such a solution means that only a person having with the appropriate key, password or PIN can access the contents of the disk. For such a user, the access is transparent. On the other hand, the acquisition of a drive by a person without a key (for example, following a theft) only makes it possible to view the data in encrypted form. Full disk encryption is available in all modern operating systems, often in the form of a native tool (e.g. Bitlocker in Windows, Filevault in Mac OS) or a corresponding option in the security panel. It is important to make sure that the solution is applied correctly. It also means that a sufficiently strong key has been chosen, or a complex, hard-to-guess password or PIN. If it is possible, it is always safer to use passwords than numeric codes. It is important to remember that the cost of encryption is a slight decrease in system performance due to the need for additional resources. It is also essential to take proper care of the encryption key.

[56] The so-called drive-by download http://en.wikipedia.org/wiki/Drive-by_download

The principle of data encryption also applies when data is stored outside the device – on portable drives or in the cloud. If this is the case, first of all full disk encryption should be considered, and if this is impossible or impractical, encryption of specific files or folders.

2.8.5. Availability of systems and applications. Backups

The CI operator should ensure the availability of operated systems and applications in a proportional and appropriate manner. One of the essential parts of this process for virtually all systems is the creation of backups. Activities can be divided into the design part and the operation part of systems and applications.

Availability[57] can be achieved through:

a. Elimination of Single Points of Failure, i.e., the part of an ICT system whose failure brings the entire system to a halt.
b. Use of redundancy at different levels (see further in this document)[58].
c. Immediate troubleshooting by system operators. If, in a duplicated (redundant) system, one of the components of one copy fails, such failure must be rectified immediately. The intervention will not be visible from the system user's point of view. Examples include replacing a drive in a RAID array or changing the telecommunications carrier.

Measurement of the availability of systems or assessing the availability of systems can be done by determining the SLA with the help of a percentage of availability time. The illustrative values are shown in the table below:

Table 8 Levels of availability according to SLA level.

SLA level	Unavailability per year	Unavailability during the day
99%	3.65 days	14.40 min
99.9%	8.77 h	1.44 min
99.95%	4.38 h	43.2 s

[57] In Polish, two completely different terms are referred to as "availability". Here we discuss a concept referred to as "*availability*", i.e. the ability to operate a system undisturbed. Another term is "*accessibility*", which means the ability of a device/system/application to be used by all potential users, including, in particular, people with various disabilities.

[58] Note: it is very common in the literature to treat the point where two copies of systems are connected as a special kind of single point of failure, which means that it is this part of the infrastructure and applications that should be especially carefully prepared.

99.99%	52.6 min	8.64 s
99.999%	5.26 min	864 ms

It is clear that the increase in availability requirements translates into the price of the solution, where with higher requirements, the increase ceases to be linear and the price increases extremely quickly. It is advisable to carefully define the availability parameter and the adequacy of the assumed parameter to the needs, because also the continued operation and maintenance of high availability can be extremely costly.

When determining the total availability, it is important to remember that it is the product of the component values, i.e. if there are two components of the system that must be considered together, the first with an availability of 99.999% and the second with an availability of 99%, the availability of the entire system is only 98.99%. This puts a question mark over the architecture of the system when the high-cost availability of the "five nines" achieved will be offset by the second component of the system.

When using external providers, it is worth verifying not only the declared (contractual) availability value but also – if such data is available – their past performance. For reputable suppliers, the actual level of availability should be higher than claimed.

To evaluate the introduction of appropriate solutions to increase the resilience and availability of ICT systems, it is useful to use the following table:

Table 9 Selection of solutions according to the type of failure.

Type of failure	Example	Examples of solutions
Failure of a single system component	Disk failure Drive controller failure	Use of drives with high MTTF value (sometimes MTBF)[59]. RAID array Driver duplication
Failure of one system	Server failure	A copy of the system in the same processing center

[59] MTTF – Mean Time To Failure; MTBF – Mean Time Between Failure. For servers, drives with higher MTTF/MTBF values are usually used. Note that this is a statistical value provided by manufacturers and does not protect against failure.

Failure of the processing center	Blackout Access network failure Local natural disaster Local terrorist attack	Redundancy of power systems Several network suppliers A copy of the system in several processing centers Emergency migration to a public cloud (cloud copy) – see Chapter 5.5
Disaster of great magnitude	Energy crisis on a national scale Coordinated terrorist attacks War Natural disaster of great magnitude	Cloud copy, including in another country, also on another tectonic plate Emergency migration to a public cloud

Assessment of the threat will allow to correctly determine the target availability and resilience of the ICT system. For the assessment, use the list of risks in Chapter 2.8.3.3. Hazard types.

An essential part of the plan to achieve high resilience and availability of the CI operator's systems is to prepare a backup process. When planning such a process, it is important to consider the possibilities presented earlier to increase availability and two parameters related to backup.

a. RTO (Recovery Time Objective) – the maximum acceptable time of system unavailability.
b. RPO (Recovery Point Objective) – the maximum acceptable time during which data entered into the system was lost.

It should be understood that ensuring high system resilience and availability by other means does not relieve the operator from creating backups. Their creation can be related to the use of in-house infrastructure, hosted infrastructure or a public cloud.

As a minimum of protection, it should be assumed that the backup – regardless of the medium used – must be physically distant from the system, depending on the evaluation of the necessary physical protection (cf. the risk table above)! An analysis of other risks (cf. Chapter 4.3) should lead to proper protection and storage of backups.

For archiving purposes, as well as for process accountability purposes, both by law and internal retention policies, the CI operator should prepare a policy for creating and storing more than one consecutive backup.

It is recommended that in the context of critical data, additional backup storage methods (e.g., in another provider's cloud or on-premises) should be used.

2.8.6. Emergency Cloud Migration Plan

Experience from the war in Ukraine has shown that CI operators' IT assets have become the target of hybrid attacks including cyber and physical threats. The practical solution was to migrate resources, data and systems to the cloud, particularly to a cloud located outside the country. Numerous examples have shown that such a migration of resources can be carried out quickly and efficiently, including under wartime conditions, although in the absence of prior preparation the technical solutions will not be optimal and many problems may arise. In order for the emergency migration process to be carried out efficiently, it is recommended to prepare an Emergency Migration Plan, preceded by the preparatory process described below. **Emergency Cloud Migration Plan** should be an integral part of the resilience ~~CI protection~~ plan.

When preparing the Emergency Cloud Migration Plan, a CI operator should first evaluate which cloud will be usable, including government cloud, community cloud or public cloud. If a cloud other than the public cloud is chosen, the CI operator should agree with the cloud managers on the formal and physical possibilities for such migration, so that the necessary resources are available to the operator. The Emergency Migration Plan in such a case should be jointly prepared or formally reviewed and confirmed by the managers of the government cloud or community cloud. If emergency migration to the government cloud or community cloud is not possible for formal, organizational or technical reasons, emergency migration plan to the public cloud should be prepared. The following chapter mainly discusses the principles of preparing an Emergency Migration Plan to the public cloud because the capability assessment and evaluation of public cloud providers can be prepared by the CI operator without the need to cooperate with the provider, or – with all criteria met – several providers can be selected for the actual migration.

The benefits of migrating to the cloud:

a. Immediate availability – the migration process can be initiated as soon as the threat is recognized or after the appropriate alert is issued by the relevant authorities.
b. Security – reputable cloud providers provide safety and protection often at a higher level than is the case with CI operators' own infrastructure.

c. Dispersion under the control of the CI operator – they can decide where each system and data will be located. Even using a single location (one region) of the public cloud will increase security, but the Emergency Migration Plan may provide for further dispersion (including the creation of dummy targets), which will become an additional difficulty for the attacker.
d. Choice – the operator can choose from a number of public cloud providers; cloud companies from NATO and EU countries, as well as Polish companies that are technology leaders.
e. Scalability – the resources of cloud providers far exceed the needs of all CI operators simultaneously. [60]
f. Flexibility and management of the migration process – it is up to the CI operator to decide what, how and for how long will be moved to the public cloud.

Preparation of the **Emergency Migration Plan** to a public cloud should begin with the preparation of an assessment of capabilities and necessary resources (preparatory process). The operator should make use of standardized and already prepared materials, lists of questions and procedures, if they are available.

Preparatory process – own resources

a. Personnel – at a minimum, an assessment should be made of:
   - own resources (personnel, qualifications) necessary for emergency migration,
   - the possibility of obtaining additional external personnel, especially in a crisis situation affecting a larger number of entities at the same time,
   - the availability of processes for upgrading personnel skills in operating with cloud computing,
   - the availability of a process for upgrading the skills of security personnel responsible for cloud security.

b. Applications – at a minimum, legal (including licensing), organizational and technical conditions should be evaluated:
   - opportunities to migrate currently used applications and systems to cloud technologies (e.g., moving applications to a private cloud, containerization, also: migration to a public cloud),
   - opportunities to implement new solutions using technologies used in a public cloud computing, including public cloud,
   - (if cloud solutions are already used by the operator) the possibility of changing the location (changing the cloud region) for a given application and the process that accompanies it. Consider the potential change of provider, e.g., a

[60] An example of the scalability of cloud computing was the transition during the pandemic from workplace and school work to online work. In literally days and weeks, entire industries moved operations to the cloud. It is estimated that from March to June 2020, in education alone, the number of people working and learning online using cloud platforms every day increased from several thousand to more than five million!

domestic provider with data centers exclusively in the Republic of Poland to an international provider.

b. Data – at a minimum, legal, organizational and technical conditions should be evaluated:
   - conditions for processing in the public cloud, in particular for personal data,
   - additional safeguards for data processed in the public cloud, such as required encryption methods, required key storage methods, among others,
   - additional security in the form of cloud backups.

c. Authentication – at a minimum, an assessment should be made of:
   - the ability to unify authentication for the current and cloud-based solution,
   - checking the possibility of using multi-factor authentication,
   - user access monitoring tools.

d. Other
   - exclude from the Emergency Migration Plan systems that process classified information, [61]
   - determine the minimum time to maintain duplicated resources in the cloud (used to determine potential maintenance costs after migration),
   - review and evaluate current service and support contracts with IT suppliers.

Preparatory process – evaluation of public cloud providers

The CI operator performs risk analysis and evaluation of public cloud providers. If a recommendation[62] or a risk and assessment sheet pre-prepared by the relevant regulator is available, it is necessary to use this document or verify at least the items in accordance with the following list. The risk analysis and assessment process should be formalized and documented. In the absence of sector-specific recommendations, the CI operator may use recommendations available for other sectors, treating them as a set of best practices.

It is recommended to conduct the analysis in a team consisting of representatives of the IT department, safety department, Data Protection Officer, finance department and legal department (among others, for the purpose of determining the legal risk of emergency migration to a cloud located in third countries). Keep in mind that the formal requirements for emergency migration processes to the cloud apply to an emergency

[61] Under the current legal framework, it is not possible to process classified information in a public cloud. However, there should be readiness for the potential transfer of systems handling CLASSIFIED information, should the law change or be temporarily suspended in times of threat. It is worth noting that some EU countries allow the processing of classified information in public clouds after the verification of applications, the definition of organizational and technical requirements, and the issuance of the appropriate certification.

[62] An example of a regulator's recommendation, here for the financial sector, could be the "Communication from the Office of the Polish Financial Supervision Authority regarding the processing of information by supervised entities in public or hybrid cloud" of January 23, 2020.

situation, and therefore may be different than those imposed on a cloud solution in a normal situation. It can be assumed that a cloud solution that meets the criteria for a normal situation will also meet crisis requirements.

The risk assessment may be different for different systems and applications with the same information from the cloud provider (example: locating the data center in a non-NATO EU country, e.g. Austria, may be more important for certain scenarios, while locating the CPD in a non-NATO EU country, e.g. Canada, may be more important if it is advisable to create a duplicate application outside the European continent for security reasons).

Analysis of public cloud service offerings

a. The provider makes available, also in electronic form, a formalized contract and other documents such as terms of service, regulations, certificates of compliance with standards, post-audit reports, etc.,
b. The documents make it possible to clearly determine the governing law for the contract with a public cloud provider,
c. The documents allow clear division of responsibilities in terms of security, continuity of service delivery, SLA level,
d. The documents or administrator tools [63] allow to determine the location of the [64] provider[65] data processing center,
e. The documents make it possible to clearly identify the ownership of the processed data during the term of the contract as well as after its termination,
f. The documents allow the user to see the list of sub-providers (if any) and indicate how to communicate it when new sub-providers are added,
g. The documents clearly indicate that it is possible to audit the provider, and that the provider regularly undergoes audits performed by independent auditing bodies, as evidenced by appropriate certificates – verification of compliance with at least the following standards is recommended:
    - ISO 27001 – information security management systems,
    - ISO 27017 – an extension of ISO 27001 for information security controls for cloud services,
    - ISO 27018 and/or ISO 27701 – management and protection of personal data in cloud services,

[63] Many public cloud providers allow users to choose their data center or region – the final decision is made by the users themselves.

[64] Public cloud providers often use the term "region", which refers to an area containing at least two (usually three) data centers where data storage and processing take place. A public cloud region usually aligns with a country's borders, although larger countries often have more than one region.

[65] Precise indication of the address of the data center(s) is rarely provided for security reasons – the minimum requirement is to indicate the country in which the data processing center or region of the public cloud provider is located.

- ISO 22301 – business continuity management systems,
- SOC 1 and SOC 2,
- ISO 50600 min. class 3 (data center facilities and infrastructures) or ANSI-TIA 942 at least Tier 3[66],
- (optional) NIST 800-53 at least R4[67],

h. The provider applies Zero Trust[68]principles, in particular:
   - the default principle of no access to cloud user information,
   - the default principle of no administrator account in the launched resources (access is granted for a limited time, within the necessary scope of authorization),
   - encryption of data, both during storage ("at rest") and during transfer ("in transit") – it is recommended to check the information on available methods for encrypting,
   - the possibility of introducing multi-factor authentication,
   - limits access at network-level to only the necessary connections,
   - restricts access at the device level to permitted devices only,

i. the provider (optionally) enables connection to the cloud via dedicated links,
j. the provider has a plan for the continuity of service,
k. the provider enables and recommends creation of dedicated business continuity plans at the application and solution level,
l. methods and tools to increase the resilience of the cloud system (redundancy, duplication in different regions) are available for the CI operator's decision,
m. the provider has a branch in Poland (recommended),
n. the provider offers professional services that can support the emergency migration process,[69] particularly a technical support program (recommended),
o. the provider has a qualification program available in Poland, i.e. training, training centers, certified trainers, formal certifications (recommended).

It is recommended that an **Emergency Migration Plan to a Public Cloud** be prepared and included in the resilience ~~CI security~~ plan, comprising at a minimum:

a. a list of systems and applications that should be moved to the cloud (duplicated in the cloud) and the data associated with them,

[66] If it is used by cloud service providers – if not, the application of SOC 1 and SOC 2 standards should be verified.

[67] The Polish Cloud Cybersecurity Standards (SCCO) are *de facto* translated provisions of NIST 800-53 R5.

[68] Compare section 4.1. Also: a potential verification is that the provider implements NIST 800-207, but this is not yet a widely used standard, especially in Europe (NIST are US standards).

[69] If required by the nature of the emergency migration process for certain systems and applications, it is recommended to verify that the provider has professional services staff with the appropriate security clearances, as well as that the provider holds an Industrial Safety Certificate.

b. determination of the priority (order) of migration of systems and applications,
c. determination of the scope of migration for each item on the list, from a minimum of cloud backup (data copy), to full functionality of the system or application served from the cloud (full migration),
d. (if necessary) identification of additional tools to increase resilience and security for specific items on the list,
e. the composition of the team responsible for the migration with an indication of the roles and responsibilities of individual team members,
f. in particular, the team in charge of the migration must identify the person(s) responsible for contacting the public cloud provider and overseeing the implementation of tasks,
g. a list of external personnel necessary or recommended for the execution of the migration process, including, in particular, the possibility of obtaining professional support from the provider and domain providers, if necessary,
h. pre-selection of countries and cloud provider regions to which migration [70]is anticipated,
i. identification of at least two public cloud providers (first choice, second choice) selected on the basis of the supplier evaluation performed in the preparatory phase,
j. preliminary estimation of migration time and costs,
k. an assessment of internal needs within 12 months of the Plan preparation aimed at increasing the certainty of migration execution, in particular, a program for improving personnel skills, migration exercises, identifying systems and applications that should be better adapted to migration needs, changing licenses for software (if necessary), etc.

Documentation from the preparation process does not have to be included in the **Emergency Migration Plan to a Public Cloud**, however, it should be available for re-verification. An exercise involving migration to the cloud of non-production systems is recommended. It is recommended that the Migration Plan be reviewed and renewed at least every two years.

2.8.7. Software

The principles of ensuring software security are based on universal principles that also apply to ensuring safety of other ICT resources, most importantly the operating system.

The most important elements (foundations) of ensuring software security are:

[70] In emergency situations, competent state authorities may indicate preferred migration directions.

- testing software in a dedicated environment, prior to production deployment,
- operating system update,
- software update,
- testing changes resulting from updates,
- code security audit,
- cooperation with software provider.

Figure 14 Basic elements of software security.

2.8.8. Infrastructure

2.8.8.1. Networks and architecture

Separation of the network directly supporting CI from the organization's core Internet network (physical and logical)

With both virtual local area networks and firewalling, one can create a solution of separating the network directly supporting the organization's CI. A network directly supporting CI is understood as that part of the organization's network where key data is processed and facilities, equipment, installations that constitute the relevant CI are operated. This part of the network should be subject to special protection, so in practice one should apply all of the discussed safeguards in a supplementary way just to this part of the network. The configuration of these safeguards should be implemented at the highest and most restrictive level.

In order to ensure the separation of the CI network from other networks in the organization, it is recommended to implement network segmentation according to the model shown below (after adjusting to the needs of the organization).

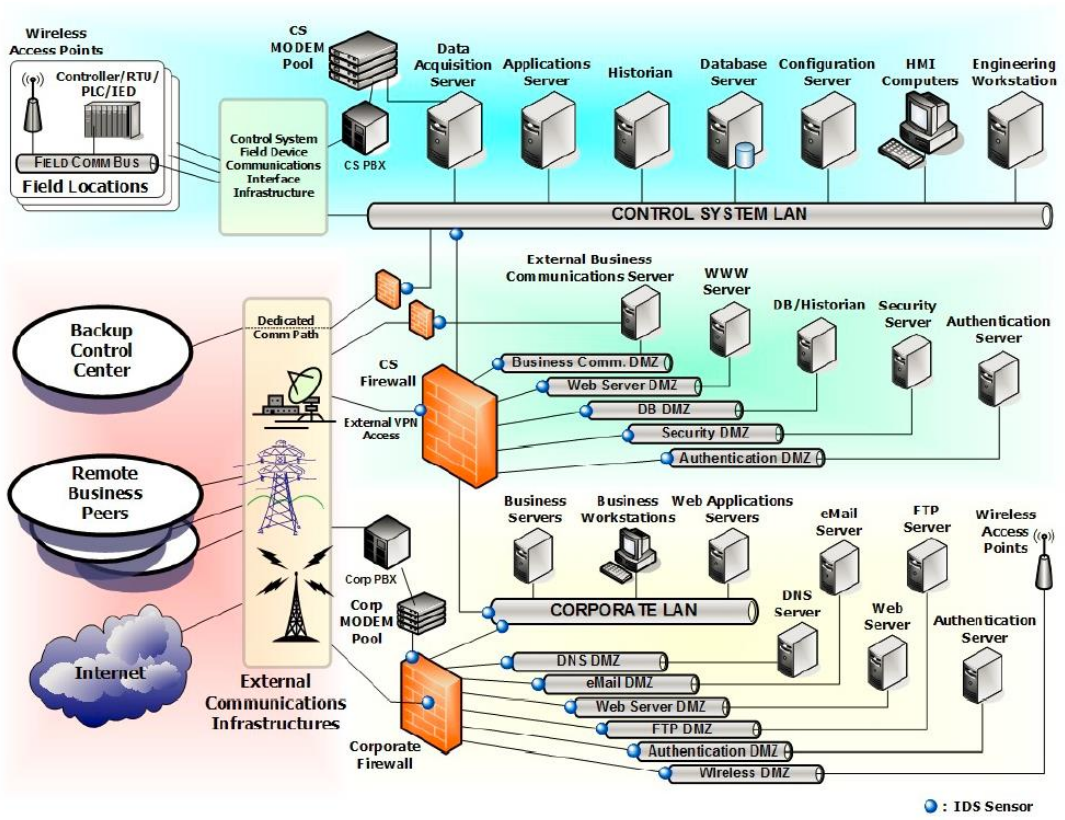


Figure 15 Network segmentation model[71].

The above model assumes the creation of isolated safety zones. Communication between zones is controlled and limited to the degree of security required for the zone. Automation systems (understood as SCADA systems, DCS, control layer devices, and control and measurement apparatus) should be included in the highest level of security due to their direct impact on CI service continuity.

An additional demilitarized zone (DMZ) should be created between the CI networks and other networks. All traffic to and from the CI network should use intermediary solutions placed in this segment (e.g., proxy servers, dedicated databases, file servers). Any direct connections between the CI network and other networks in the organization, bypassing the DMZ segment, should be blocked.

All network traffic passed into the DMZ segment and from that segment to the CI asset network should be strictly controlled using firewalls. In addition, in order to protect against attacks and detect malware, network traffic should be controlled using IDS/IPS solutions.

[71] NIST Publication 800-82 rev. 1.

2.8.8.2. *Wireless networks*

Wireless networks, due to their ease of construction and configuration, and convenience of use, are very widespread. The use of wireless networks, without the use of appropriate security measures, carries great risks, in particular the possibility of:

- illegal use of these networks for criminal activities,
- unauthorized access to the information of other entities.

Wireless communication is increasingly finding its way into the automation environment, especially for installation metering, where long-distance data transmission is required. It is then necessary to pay special attention to the security of transmitted data – interception or interference with this data can directly affect the technological process.

It is also worth noting that the security of wireless networks should be considered not only from the point of view of organization's own networks, but also from the point of view of third-party networks used by employees of the organization.

Protecting organization's own wireless network

When analyzing the safe use of wireless networks, one should consider the following security foundations:

(1) **Traffic separation from wireless networks**

Disabling communications from wireless networks to networks supporting CI or resources that constitute CI is an effective way to reduce the risk of disrupting CI services.

(2) **Communication encryption**

Wireless networks should utilize communication encryption. The most popular encryption standards are WPA/WPA2/WPA3 (*Wi-Fi Protected Access*). The WPA2 and WPA3 standards are more secure and are recommended. WPA3 brings a number of changes compared to its predecessors. The most important are:

- TKIP/AES encryption was modified, and in fact completely replaced with SAE encryption,
- effective mitigation of the risk of a KRAK attack,
- WPA 3 Enterprise 192 bit encryption,
- WPA 3 Personal 128 bit encryption,
- protection against Brute Force attacks – automatic lockout on dictionary password cracking attempt,
- compatibility with previous versions (WPA/WPA2),
- possibility to use shorter security keys.

(3) **Broadcasting the network identifier**

The basis of a cyber attack on a wireless network is the detection of that network, so disabling the broadcast of the so-called network SSID (Service Set Identifier), while it will not provide full security, will certainly make a successful cyber attack more difficult.

(4) **Access control based on MAC address**

Only devices whose physical MAC address was previously entered as a permitted address are allowed to connect to the wireless network. This reduces the likelihood of unauthorized network devices connecting to the network without using specialized techniques to illegally clone the chosen MAC address.

(5) **Physical restriction of network access**

Improving the security of wireless networks in an organization is also possible by physically restricting access to the network, i.e. shaping the radio signal so that it is accessible only from selected locations. It is necessary to avoid a situation in which the signal is generally directed outside the location of the information. Conducting adequate threat monitoring[72] will help detect unauthorized access attempts.

Secure use of a third-party wireless network

In addition to ensuring the safe use of the organization's own wireless network, it is also important to ensure the safe use of third-party networks. These networks are mainly used by employees who are currently outside the organization's premises. The best practice is to prevent them from such accessing the organization's network, where the CI is located. Also, if employees use mobile devices that, when connected to the organization's local network, have access to critical resources, these devices should not have had prior access to external networks (both wireless and wired).

In all other cases where access to an external wireless network is allowed from company devices or for business purposes, the following rules should apply to employees:

- they should only use wireless networks they are familiar with (e.g., from a known telecommunications carrier),
- they should only use encrypted wireless networks (WPA/WPA2),
- connecting to the organization's resources (e.g., e-mail) should be done only through a dedicated, encrypted VPN channel[73],
- in the case of not using wireless networks, they should disable the wireless network card installed in the mobile device.

[73] See section 2.8.3.4 Access control (external access).

2.8.8.3. *Event monitoring*

Regardless of how securely particular IT network is protected, the possibility of a successful cyber attack always exists. Therefore, the organization should conduct continuous monitoring of threats.

Types of monitoring systems

The following types of devices can be used to set up a threat monitoring system and enable an early response to incidents.

- Intrusion Detection Systems (IDS)

  These are real-time cyber attack detection systems. The detection is based on a known network cyber attack pattern (known as a signature) or the detection of anomalies in network traffic. The advantage of such systems is that they can detect cyber attacks that are able to penetrate firewall-type protection through more detailed analysis of network packets (e.g., network worms, cyber attacks on services and applications, or unauthorized login attempts). A typical IDS consists of a central system, one or more sensors, and a database for processing the collected logs. Two types of IDS-type systems are possible:

  - Host Based Intrusion Detection System (HIDS) – a network threat detection system designed for selected devices (such as key servers),
  - Network Intrusion Detection System (NIDS) – a network threat detection system designed for selected networks (it can be located, e.g., at the interface between the local network and the Internet).
- Intrusion Prevention System (IPS)

This system is similar to an IDS, with the same division between systems installed on a specific device (HIPS) and on a network (NIPS). The main difference is that while an IDS alerts a user to a threat, an IPS is able to take active system protection action, such as blocking traffic from a specific source address.

IDS and IPS systems can be used complementarily. When deciding to use both systems, it is good practice to place the IPS at the network interface so that it actively protects against a wide variety of new cyber attacks, including cyber attacks that have just appeared on the network and their signatures are not yet known, and detection is done by anomaly detection (so-called *Zero-day attacks*). An IDS, on the other hand, can be used mainly inside the network, behind the firewall so that it monitors and alerts for exploits on the internal network without active blocking action. Also to be considered is the implementation of a SIEM-class tool (Security Information and Event Management), which collects information and correlates events from all relevant systems and detects behavioral anomalies.

Monitoring principles

Threat monitoring should be established to protect the company's critical assets. The standard deployment of appropriate monitoring systems should cover the following logical locations within the organization's network:

- the interface with the Internet network,
- the interface with the network in which management takes place (within the internal organization),
- key CI-supporting devices.

In addition to the undoubted advantages of operating IDS-type systems, there are also disadvantages. One of the most significant disadvantages is the transmission of false alarms by monitoring systems. There are two types of such attacks:

- *false positive* – false alarm when there is no real threat,
- *false negative* – no alarm in a situation where there is a real threat.

The issue of false alarms is particularly important as their frequent occurrence (primarily *false positives*) can lead to ignoring such alerts, and consequently failing to respond to an actual cyber attack. Therefore, an important task when using monitoring systems is to configure them to a state that minimizes the occurrence of such errors[74].

In addition to the implementation of monitoring systems, a proper procedure for operating these systems must be developed. The most important elements that should be included in such a procedure[75] are:

- ensuring that any monitored network devices, as well as the monitoring systems themselves, have a unified operating system clock time,
- constant monitoring of alarms signaling threats,
- verification to ensure that all systems requiring it are covered by the monitoring system,
- ensuring the security of devices used for monitoring,
- forwarding alerts on particularly dangerous threats to the incident handling system.

---

74 When it comes to techniques for improving configuration, it is worth consulting the advice provided at http://www.symantec.com/connect/articles/strategies-reduce-false-positives-and-false-negatives-ids

75 Further information on the principles of monitoring and auditing procedures can be found ate http://www.isaca.org/Knowledge-Center/Standards/Documents/ P3IDSReview.pdf

Detection of unwanted network traffic

Due to the limited effectiveness of antivirus software, especially in dealing with targeted threats (e.g. APTs), it is recommended to monitor network traffic for characteristics of malware activity. By detecting traffic to identified "bad" areas of the Internet, it is possible to conclude with high probability that an infection has occurred on the network – regardless of what malware is used and whether it is detected by an antivirus. Suspicious activity can be detected in at least two ways – through DSN queries and at the IP layer. In every case, the amount of collected data may prove to be a barrier. This is because it is necessary to ensure adequate bandwidth and disk space for data transfer and storage, respectively.

DNS query monitoring

Queries for specific domain names sent by devices on the local network to the DNS server can be compared with lists of known malicious domains published by threat monitoring services and provided as part of security services by external entities. In the case of detecting communication with a suspicious domain, actions of varying levels of invasiveness can be taken – from triggering an alarm in the monitoring system, to blocking name resolution (e.g., using DNS blackholing), blocking connectivity (e.g., by modifying firewall rules), to redirecting traffic (e.g., to a sinkhole).

It is also advisable to archive DNS queries from the local network, as the ability to analyze them is an invaluable help in the event of detecting an intruder. Often, based solely on historical DNS query data, it is possible to determine how malicious software infiltrated the network and which resources it accessed

DNSSEC (Domain Name System Security Extensions) is an extension to the DNS protocol that enhances its security. DNSSEC creates a secure domain name system by introducing cryptographic signatures. They are added to already existing DNS records. DNSSEC is based on public key cryptography, certificates and digital signatures. DNSSEC provides additional authentication and data integrity. It protects against cache poisoning and can also protect additional information using TXT records. Implementing DNSSEC also impacts issues related to DDOS attacks and can cause challenges when implementing zone delegation. DNSSEC does not address privacy issues related to DNS data.

IP traffic monitoring

To collect data on all IP-layer communication with external networks, the NetFlow mechanism can be used, gathering information from network devices such as source and destination IP addresses, ports, and protocols for the packets passing through those devices. NetFlow-compliant solutions are supported (under various names) by most network device manufacturers, and dedicated tools – including free ones – can be used

to analyze the data collected in this way. Note that some devices (at least in the default configuration) do not analyze all packets, but only a certain statistical sample. Sampled data may be sufficient for monitoring traffic volumes on individual services, but definitely not sufficient for detecting malicious connections. As with DNS queries, archiving NetFlow data can be very helpful for incident investigation.

2.8.9. Industrial automation security

The control layer of the ICT systems environment model includes devices which collect information from the field instrumentation (i.e. sensors, protection devices, meters, signaling devices) and which directly control actuators (e.g. pumps, valves, drives). Most of these devices are critical assets for the supported processes and should be subject to special protection. Note that the integrality of the software distributed by the supplier of controllers should be a responsibility of the supplier.

2.8.9.1. Security of PAC/PLC/RTU and other programmable devices

PLCs (Programmable Logical Controllers) are programmable devices used to control and/or monitor process systems. PLCs can be combined into larger systems through integration using industrial networks. PLCs most often exchange data with other controllers and master monitoring and control systems (e.g. SCADA systems). Note that recently there has been an evolution of the PLC concept towards a common hardware platform, performing many more tasks than just typical control algorithms. Such advanced devices are referred to as PAC (Programmable Application Controller).

RTUs (Remote Terminal Units), like PLCs, send data to master systems (e.g. SCADA systems). They are most commonly used in power sector and other geographically distributed systems to transmit telemetric data.

A specific area of PLCs/PACs/RTUs application are safety systems, also referred to as SIS (Safety Instrumented System). The role of safety systems is to bring the process to a state that is considered safe by, for instance, emergency shutdown, through the so-called ESD (Emergency Shut Down) systems. It is recommended that such systems operate in parallel and completely independent of the primary control system and use dedicated, specially certified components.

PAC/PLC/RTU devices must be protected from unauthorized physical access by being placed in locked technical rooms. Access to the rooms should be controlled (procedurally or with technical security measures). The devices should be placed in lockable electrical cabinets equipped with technical solutions to stabilize environmental working conditions (e.g., ventilation, air conditioning, heaters) and provide protection against dust.

Access to the PAC/PLC/RTU device software should be protected by a unique password. It is recommended to use a unique password for each device. Passwords should be changed periodically in accordance with the company's security policy. It is recommended to immediately change the password after: the end of the start-up stage, a change of job duties or when people with access to device softwares leave the company, suspicion of unauthorized access to the password or device. It is especially important to

change the default passwords of manufacturers/suppliers. Using (leaving) these passwords is a vulnerability that can be taken advantage of by potential attackers.

In order to carry out diagnostic works or changes in the configuration of devices, it is recommended to use dedicated engineering stations (portable ones such as laptops/programmers or stationary ones, that is of desktop type). Engineering computers should not be used for other purposes, in particular, they should not be connected to the office network or to external networks. Transfer of files to engineering stations should be done only after they have been checked by up-to-date antivirus software. It is recommended that third-party maintenance personnel do not use their own engineering stations (due to limited control over their security).

CI operators using PACs/PLCs/RTUs should strive to ensure that they have a set of up-to-date copies of device software:

- in editable versions with access to all software blocks (except for blocks predefined by the device manufacturer),
- containing a set of developer's comments with a level of detail sufficient to clearly identify the role of individual software fragments,
- names and descriptions of variables,
- definition of hardware configuration.

Failure to have a copy of the software that conforms to the requirements specified above increases the organization's dependence on the automation system supplier and can significantly increase the cost and complexity of any changes to the control algorithm.

Any changes to the software of PAC/PLC/RTU devices should be made with the assurance that the original application can be quickly restored. Before launching a new software, it is recommended to conduct functional tests on a simulator or in a dedicated test environment. The above comments relating to PAC/PLC/RTU devices also apply to field devices, typically managed by programmable controllers. This is due to the fact that an increasing number of inverters, motor protections, distributed I/O systems and measurement systems allows not only simple configuration, but also the programming of specific action algorithms in case, for example, communication with the master controller is lost and autonomous operation is required.

2.8.9.2. *Security of HMI devices*

In the immediate vicinity of process systems, local operator panels, HMI (Human Machine Interface) stations are often installed. Their purpose is to enable continued supervision and control of the technological process in the event of communication link failures, and to streamline maintenance works by providing local access to information on the status of the process, system and automation system components. These stations,

placed in areas that are seldom used by personnel, can be a point of unauthorized access to the automation system.

The HMI stations should be protected from unauthorized physical access by placing them in locked rooms or field cabinets where access is strictly controlled. The devices should be installed such a way that the operator or other people in the room could have access to the user interfaces only (screen, keyboard, mouse, etc.). The device should be protected against access to the physical ports of the device.

All recommendations regarding password security and changes as indicated in the chapter on PAC/PLC/RTU devices apply to HMI stations.

Critical infrastructure operators using HMI stations should aim to secure a set of:

–up-to-date, editable copies of HMI applications,

–user manual, understood as both instructions for operators and a technical part for service/control system engineers, including information on the structure of the application.

2.8.9.3. *Security of industrial control networks*

Specialized communication protocols are used in the area of the control and I&C (Instrumentation and Control) layer. Some of these protocols were designed many years ago without taking into account the requirements arising from modern ICT threats. There are known vulnerabilities in these protocols that can be used to disrupt operation or take control of critical infrastructure. It is recommended to secure industrial control networks using protocols having known vulnerabilities by:

- limiting physical access to network infrastructure,
- limiting logical access by implementing appropriate security mechanisms at higher layers of the network segmentation model,
- where feasible and economically justified (e.g., many years of system operation are anticipated), migration to communication protocols that provide a higher level of security should be considered.

Security of SCADA system/DCS operator stations

Industrial master monitoring and control systems, such as SCADA or DCS, for data storage and processing and user interface implementation, increasingly use the same technical solutions as other IT systems (including: servers, operator stations, disk arrays, standard operating systems, TCP/IP networks). Security rules for these solutions were described in earlier chapters. Note, however, that the focus on ensuring maximum system availability forces a different approach to the practical implementation of security requirements in some cases, e.g., where SCADA systems/DCS are the primary method of technological process supervision and control, securing access to operator

stations with password may not be advisable due to the risk of error when entering or forgetting the password by the operator in a high-stress situation. In the case of such systems, the required level of protection against unauthorized access is provided through restrictively limiting physical access to the control room.

Installation of an operating system patch, even one responsible for fixing critical security errors, may not be installed on components of systems responsible for supervision and control of industrial processes unless it is certain that the installation will not interfere with the operation of that system. In such cases, temporary physical disconnection of the control system's network from other ICT networks is often selected until the patch operation is tested by the control system manufacturer or in own test environment.

2.8.10. Contingency plans and recovery procedures

2.8.10.1. Process of creating and improving plans

Contingency plans ensuring the recovery and continuity of IT infrastructure operations should be prepared and maintained according to the presented scheme.

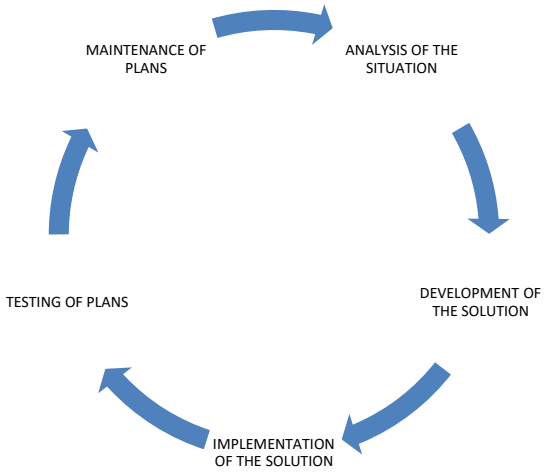


Figure 16 Cycle of implementation of contingency plans.

Analysis of the situation

In this phase, the most important task is to determine the resources required for a smooth and safe switchover/recovery of IT systems. This is a task closely related to the risk assessment, the required recovery time objective (RTO) and the acceptable recovery point objective (RPO); the RTO and RPO parameters directly affect the backup technology. These resources can be either personnel, technical infrastructure, or

external resources, such as key suppliers of materials or information needed to maintain business processes and support. Also in this phase, the criteria need to be defined for triggering contingency plans (drawing the line between contingency plans and incident management).

Development of the solution

The development of the solution phase produces detailed plans that answer the questions: when? who? what? how? When developing these plans, it is important to remember that not all situations can be predicted in the planning phase. Therefore, in addition to detailed ready-made plans, there should be a mechanism for resolving a situation when something that no one predicted has occurred. Such a mechanism, first of all, should include rules about which people (positions) are involved in solving the problem and how they make a decision.

An important part of securing data is the systematic creation of backups, the frequency of which should be based on risk analysis and the time of data availability. The scope of backups for servers must include system software (system configuration), installed application software. In case of network devices (routers, switches, firewalls, etc.), this means storing their configurations, and for workstations, this is processing of information according to the user's request. It is important to remember that backups should not be stored in the same place as the systems for which they were made (the physical loss of a building, such as a fire, means in this case both loss of the system and loss of the backup). Backups should be encrypted and periodically tested (whether it is still technically feasible to read data from the carrier).

Implementation of the solution

The development of the contingency plans should be followed by their implementation. The right thing to do is to test the planned solutions along with the implementation. It is not a matter of full testing, just to see if the plans are complete, procedurally logical and feasible. This can be done by the implementation team.

Testing of plans

The actual verification of the plans takes place during the testing phase. In this case, all interested parties participate in the testing. These tests can be more or less complex. A simple test can consist of running a single emergency procedure (a simple test can be carried out independently by IT units without any involvement of business units). A complex test, on the other hand, should include the launch of several emergency procedures at once and its coverage should extend to the maximum number of the company's organizational units (active involvement of business units in verifying the quality and correctness of the recovery of IT systems in the backup location). In cases

where it is not possible to test a specific scope, tests involving practicing a theoretical plan, with various scenarios, can be a solution.

In practice, the group involved in the plan implements selected scenarios "on a piece of paper" (so-called table exercises) or in a separate, isolated test environment. Such tests in the aforementioned areas help consolidate correct behavioral mechanisms. An example scenario might include:

- failure of the organization's main mail server,
- virus attack disabling alarm messages transmitted from the SCADA system,
- failure of the building's physical access control system.

As a result of testing, a detailed report is prepared, which should include information on:

- emergency situation,
- test execution,
- achieved results compared to expected results,
- analysis of the reasons for the differences (if any),
- proposed corrective actions(if necessary).

Once the tests are completed, the proposed corrective actions presented in the report are implemented and the contingency plans are finally approved.

Maintenance of plans

Maintenance of the contingency plans consists of two main activities:

- training of those responsible for actions during a crisis situation,
- testing of approved contingency plans.

It is advisable that both training and testing take place at least once a year.

Of course, if a change occurs in the environment in which the organization operates, such as the arrival of a new system or the establishment of a new organizational unit, the entire cycle of creating contingency plans should be repeated. If no such changes occur, it is worth repeating this cycle at least once every 2 years.

2.8.10.2. *Response to incidents*

Basic recommendations for detecting and responding to targeted attacks (including APT).

Efficient threat response is a key element when it comes to countering targeted attacks, including APT (Advanced Persistent Threat). The targeted attack means an attack on a specific organization or person (or group of organizations/persons). An APT attack is a

subset of this attack category and refers to threats (organizations) that have advanced capabilities to carry out an attack, both at the technical and organizational, financial and developmental levels, and have clear long-term goals they will systematically pursue.

The assumption must be made that sooner or later there will be a successful intrusion into a protected network. The establishment of the response team's work and plans should be preceded by a risk analysis which will focus primarily on determining the most important assets that need to be protected and also on defining the likely attack paths to those assets. In particular, it is worth noting the various social engineering methods which, along with the use of malware, can be used to attack individuals or departments within a company:

- spear phishing - an attack targeting a specific organization or person/group of people, when the attacker sends correspondence claiming to be a trusted institution or often a high-ranking person from the attacked organization; the purpose of the attack is to get the victim to execute a command contained in an email (e.g. open an attachment or visit a website provided in a link), and consequently infect the victim with malware,
- clone phishing - cloning a real e-mail message. A criminal may use a template while creating a new one and add modified links to a malicious website. The victim is convinced that they are receiving an identical message from the same sender,
- whaling - a type of personalized attack designed to capture data from persons holding top positions in the company,
- brand phishing - scammers impersonate an enterprise providing services to the company under attack,
- waterholing, watering hole attack - a targeted attack where the attacker identifies websites visited by victims (e.g., subcontractor websites, knowledge providing systems) and then, through a separate attack, places malicious code in them to infect victims,
- spoofing - a type of phishing that involves domain forgery. The cybercriminal impersonates an existing domain to make their e-mail look like an original message from the chosen organization,
- smishing - an attack that uses SMS messages containing a malicious link.

Determining the paths of potential attacks will make it possible to consider various attack detection methods corresponding to the next stages of intrusion. For this purpose, it is worthwhile to become familiar with the concept and methodology of the "intrusion kill chain" introduced by Lockheed Martin[76].

[76] http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

Recommendations:

- Do not click on suspicious links and downloads in messages. You should investigate the credibility of a given message, for example, by calling the sender to whom the e-mail refers.
- The message seems urgent and arouses curiosity? The sender tempts that there are only 20 minutes to claim the prize or discount? This is one of the social engineering techniques to encourage quick and reckless responses. A huge number of phishing attacks is designed to stir up strong emotions.
- Criminals care about the realistic appearance of their websites. They are often confusingly similar to the original they impersonate. A green padlock next to the address does not guarantee that security is assured. HTTPS only means that data is transmitted securely, but it does not guarantee the reliability of the website itself.
- Do not respond to any e-mail that appears suspicious. Ignore requests for a login and password, personal information or a scan of an ID card.
- Do not trust messages containing requests for money, even from close associates or friends. Their account may have been hacked and used against their intentions. This is in particular true of social networks.

Response plans should take into account communication with external entities, including the Police and other services, network service providers, CSIRTs and also the media. It is worthwhile to verify in advance what are the capabilities of the above to provide assistance and prepare appropriate communication methods.

A correct response to a given incident requires an entity to have a good situational picture of how its own network is functioning, particularly in the context of security incidents. It is advisable to adopt a proactive attitude, that is, to proactively search for potential problems on the network, so as to be able to respond to an incident at an early stage of its development. The assumption should be made that the network may have already been compromised and focus should be placed on indicators that may prove the presence of an intruder inside the network, such as data exfiltration. The basis is the logging of network traffic for further analysis (including post-intrusion analysis). It is recommended in this case, as a minimum, to include a netflow mechanism to collect and store all network traffic for a certain period of time (optimally at least one year) and also to log all queries at the DNS level.

In order to improve the situational picture, it is recommended to read and adapt to the recommendations of the two ENISA reports:

- Proactive Detection of Network Security Incidents https://www.enisa.europa.eu/activities/cert/support/proactive-detection
- Actionable Information for Security Incident Response https://www.enisa.europa.eu/activities/cert/support/actionable-information

These documents describe methods, tools and standards for exchanging the information necessary to proactively detect threats and share information about them.

It is also recommended to use existing mechanisms for sharing data on threats introduced in Poland. In particular, it is advisable to join the existing system aggregating network security incidents involving Polish entities: such as the n6 platform created by CSIRT NASK. As part of this system, you can receive free information about threats detected on your own networks (including information about targeted attacks and APT), without having to install any software or probe. For more information about this system and how to join it, visit http://n6.cert.pl You should also consider joining the discussion list dedicated to the project: n6 forum.

2.8.11. Support in emergency situations

2.8.11.1. Security Operation Center

An important organizational issue is the establishment of an ICT security breach response team called the SOC (Security Operation Center) within the organization. Such a unit is not mandatory, but nevertheless the decision to establish it and have it functioning is worth considering. Practice shows that this type of unit, in addition to performing key tasks entrusted thereto, i.e. handling incidents, also provides excellent support for carrying out other tasks, such as conducting risk analysis, ICT audit or conducting awareness and education activities. This is possible as a result of constant awareness of SOC personnel of the most important and up-to-date phenomena in the field of ICT security and practical knowledge of network abuse and how to prevent it.

How to build the SOC[77].

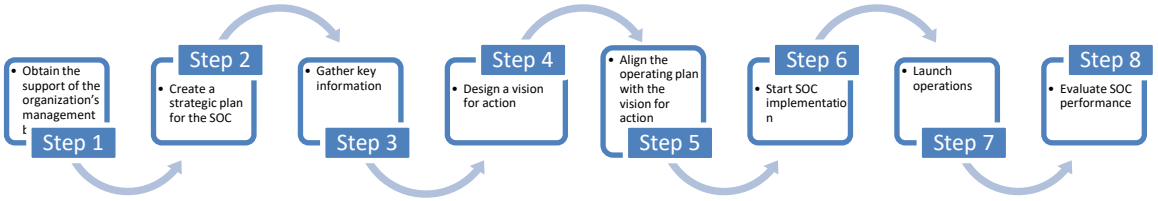


Figure 17 Stages of SOC formation.

Step 1 – Obtain the support of the organization's management board

The main task at the beginning of the journey of building the response team is to get the support of the organization's management board for such an initiative. As with any new initiative, the lack of such support may negatively affect the quality of the emerging unit.

Step 2 – Create a strategic plan

In step two, a strategy for creating the SOC should be planned in detail. What group of people will form it? What will the support from the management board look like? How to inform other members of the organization about the existence and tasks of such a team?

Step 3 – Gather key information

[77] The proposal is based on recommendations prepared by CERT Coordination Center: http://www.cert.org/

This is a very important step where we learn about the detailed expectations related to the future SOC. It is then worth discussing these expectations with the managers of other units (especially IT, legal and public relations departments). This will allow, among other things, to plan the necessary human and technical resources for the functioning of the future team. During this phase, we also gather information on the security policies already existing in the organization, including how incident response has been handled so far (if at all). Any organizational charts and organizational procedures will also be helpful.

Step 4 – Design a vision for action

While this task seems broad, it is extremely important. Defining such things as:

- the area of activity (so-called constituency) of the team, i.e. what tasks the SOC will carry out,
- determining a mission and objectives of the activity,
- establishing a scope of reactive, proactive and consultative services provided[78],
- establishing an organizational model for the emerging team,
- determining the needed resources (personnel and technical ones),
- determining budgeting sources for the SOC team.

Step 5 – Inform and gather feedback on the vision for action

A good practice when forming a team is to make sure that the detailed information about the team's vision is provided to the interested parties. This is an effective action not only from the perspective of promoting and gaining favor for the newly formed team, but also of gathering information on potential problems and risks associated with the functioning of such a planned team.

Step 6 – Start implementation

The start of operational activities involves hiring personnel, purchasing appropriate infrastructure, initially establishing operating procedures, creating a technical system to support incident handling, and preparing appropriate recommendations and guidance in the area of operations on how to behave in the event of an identified or suspected ICT security breach.

Step 7 – Announce operations

All interested parties should be informed about the commencement of the team's operations. Ideally, this will be done by a person representing the management board,

[78] The list of recognized CSIRT services is available at: http://www.cert.org/csirts/services.html

once again confirming support for the initiative. It is a good idea to then share previously developed tips and recommendations. In doing so, an attractive form of communication is recommended (e.g., a company brochure, an interview with the head of the SOC team, use of an organization's intranet).

Step 8 – Evaluate performance

After an appropriate period of operation of the team (e.g. after 6 months), there should be an evaluation of performance. This evaluation will provide an answer as to whether it was worth establishing such a unit and, if the answer is yes, what, if anything, is worth improving in its operation. To answer these questions, one can use non-measurable information, such as an evaluation survey, as well as certain metrics, such as the number of incidents reported and resolved, the time taken to handle them, the implementation of new tools to ensure ICT security, which result from the conclusions of incident handling.

2.8.11.2. *Sectoral cooperation*

A significant part of CI is in the hands of the private sector. Often organizations wielding CI are competitors in the commercial market. Nevertheless, the principle of competition should not apply to security issues. Therefore, it is advisable for organizations maintaining CI to cooperate with each other. Ideally, this cooperation is carried out within specific sectors, such as the energy sector or the banking sector.

The formula for sectoral cooperation between interested organizations is often referred to by the term ISAC (Information Sharing and Analysis Center), and most often takes the form of virtual cooperation. Within such a center, information is shared about specific hazards to a particular sector and even incidents in individual organizations[79]. This allows all participants in the initiative to use this practical information in better repelling a potential cyber attack or improving the security level of their assets. It is most important that the information shared between participants is valuable and that the principles of trust and confidentiality are not violated, primarily by ensuring responsible personnel policies for those involved in the exchange of information. As part of the center's existence, it is also possible to take joint actions to improve security across the sector. One of the most interesting and very important possibilities is the establishment of a crisis information network, which, in the event of a particularly dangerous situation for one or more of the center's members, can act quickly so that the losses resulting from a crisis situation are minimized. With such a network, it is possible to:

- notify other members of a dangerous situation,
- obtain substantive support in dealing with the situation,
- take joint action to weaken the strength of the hazard.

79 This information, due to high confidentiality requirements, can be shared anonymously.

The initiative of the Ministry of Climate and Environment, the competent authority in the energy sector creating the Information Sharing and Analysis Center (ISAC), as well as the Dutch financial sector initiative called FI-SAC[80], and the American IT sector ISAC – IT-ISAC[81] can be considered as good examples of how sector cooperation works.

2.8.11.3. *CSIRT incident response teams*

In the case of not having a SOC team within the organization, we specifically rely on external support for incident response activities. In such a situation, the incident is handled by an external CSIRT according to the external CSIRT's area of operation (constituency).

In addition to formal CSIRT teams, many entities have security teams within their structures to handle incidents occurring in networks belonging to these entities, groups of companies and institutions.

Incident reporting should take place according to the area of operation indicated in the table below. One way to find the appropriate CSIRT or institution associated with a given IP address is to use the database provided by RIPE: www.ripe.net.

TEAM	WEBSITE	AREA OF OPERATION
CSIRT GOV	http://csirt.gov.pl Computer Security Incident Response Team operating at the national level, led by the Head of the Internal Security Agency	a) units of the public finance sector, as referred to in Article 9 point 1, 8 and 9 of the Act of August 27, 2009 on public finance, with the exception of those listed in Article 26 section 5 and 6 of the Act of July 5, 2018 on the national cybersecurity system; b) units subordinate to the Prime Minister or supervised by them; c) National Bank of Poland; d) Bank Gospodarstwa Krajowego;

[80] http://www.samentegencybercrime.nl/Informatie_knooppunt/Sectorale_ISACs/FIISAC?p=content
Many other such sector initiatives can also be found on the site.

[81] https://www.it-isac.org/

TEAM	WEBSITE	AREA OF OPERATION
		e) other than those listed in points a–d, and being in the area of operations of the CSIRT MON, entities whose ICT systems or networks are covered by the uniform list of facilities, installations, equipment and services included in the critical infrastructure, as referred to in Article 5b section 7 point 1 of the Act of April 26, 2007 on crisis management; f) entities referred to in section 6, if the incident relates to ICT systems or ICT networks covered by the uniform list of facilities, installations, equipment and services included in the critical infrastructure, referred to in Article 5b section 7 point 1 of the Act of April 26, 2007 on crisis management.
CSIRT MON	https://csirt-mon.wp.mil.pl Computer Security Incident Response Team operating at the national level, led by the Minister of National Defense	a) entities subordinate to the Minister of National Defense or supervised by them, including entities whose ICT systems or networks are covered by the uniform list of facilities, installations, equipment and services included in critical infrastructure, as referred to in Article 5b section 7 point 1 of the Act of April 26, 2007 on crisis management; b) entrepreneurs of special economic and defense importance, in relation to which the organizing and supervising body for the performance of

TEAM	WEBSITE	AREA OF OPERATION
		tasks for state defense within the meaning of Article 5 point 3 of the Act of August 23, 2001 on organization of state defense tasks performed by entrepreneurs is the Minister of National Defense.
CSIRT NASK	http://www.cert.pl Computer Security Incident Response Team operating at the national level, led by the Scientific and Academic Computer Network – National Research Institute	a) units of the public finance sector, referred to in Article 9 points 2–6, 11 and 12 of the Act of August 27, 2009 on public finance, b) units subordinate to government administration bodies or supervised by them, with the exception of units referred to in Article 26 section 7 point 2 of the Act on the national cybersecurity system c) research institutes, d) Office of Technical Inspection, e) Polish Air Navigation Services Agency, f) Polish Centre for Accreditation, g) National Fund for Environmental Protection and Water Management and voivodship funds for environmental protection and water management, h) commercial law companies performing tasks of a public utility nature within the meaning of Article 1 section 2 of the Act of December 20, 1996 on municipal services management, i) digital service providers, with the exception of those listed in Article 26 section 7 point 5 of the

TEAM	WEBSITE	AREA OF OPERATION
		Act on the national cybersecurity system, j) key service operators, with the exception of those listed in sections 5 and 7 of the Act on the national cybersecurity system, k) entities other than those listed in letters a–j and sections 5 and 7 of the Act on the national cybersecurity system, l) natural persons;
CSIRT KNF	https://www.knf.gov.pl/dla_rynku/CSIRT_KNF Computer Security Incident Response Team of the Polish financial sector	financial market entities recognized as Key Service Operators (KSO) within the meaning of the Act on the national cybersecurity system

Table 10 Area of operation of individual CSIRTs

2.8.12. Recommendations

Key recommendations for ensuring ICT security:

a) Use existing norms and standards.
b) Train staff regularly.
c) Share experiences and hazard information with other organizations.
d) Create and test contingency plans.
e) Manage software change (testing, updating, code auditing).
f) Assign rights only on the basis of actual needs.
g) Use security software to protect against malicious code intrusion and information leakage.
h) Protect access to admin and development tools and restrict access to source code.
i) Monitor network traffic.
j) Secure data transmitted over public networks.

k) Create your own SOC or, in the event of an ICT attack, use the services of existing national-level CSIRTs.

2.8.13. Artificial intelligence and critical infrastructure

What is artificial intelligence?
Artificial intelligence (AI), defined as the ability to deliberately and autonomously solve human-defined problems in the process of learning through digital techniques on the basis of received input data, is a rapidly growing group of technologies that mimic the cognitive processes of human intelligence. Its development is both associated with numerous economic, environmental or social benefits and generates significant risks in particular industries and areas of social activity.
In the context of critical infrastructure systems, the integrity of which is essential to maintaining economic stability, national security and the proper functioning of the state and society, the deployment of artificial intelligence technologies represents both a significant opportunity to increase the efficiency and resilience of these systems and a challenge related to potential technological, operational and regulatory risks.

2.8.13.1 Regulatory challenges

The response to the growing role of artificial intelligence and the need to ensure its safe and ethical use in the EU was the creation of a legal framework governing the development and use of AI, i.e. the adoption by the European Parliament and the Council (EU) of Regulation 2024/1689 of June 13, 2024 (hereinafter: Artificial Intelligence Act, AI Act, AIA).
The AI Act, as an EU regulation, is directly applicable in all member states, meaning that its provisions apply without the need for implementation into national law. This ensures uniform regulation of artificial intelligence across the Union and eliminates the risk of market fragmentation. At the same time, member states have the opportunity to clarify certain issues, such as national AI oversight, law enforcement or specific regulations for certain sectors. In Poland, such a regulation will be the currently drafted Act on Artificial Intelligence Systems (UC71), which clarifies the provisions contained in EU law.
The Artificial Intelligence Act is the world's first comprehensive artificial intelligence law, aimed at balancing innovation and safety, minimizing risks associated with the use of AI systems, and protecting the public interest.
The regulation's provisions do not apply i.a. to AI systems used exclusively for military, defense or national security purposes, or for scientific research and development. The AI Act does not apply either to cases in which artificial intelligence is used by natural persons for purely personal nonprofessional activities.
The regulation does not define artificial intelligence itself, but refers to the term 'artificial intelligence system.' As defined in Article 3(1) of the AIA, an 'AI system' means a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.
The Artificial Intelligence Act classifies AI systems according to the categories of risk they pose. Based on this, four main categories are introduced:

- Systems generating unacceptable risks – so-called prohibited artificial intelligence systems, described in Article 5 of the AIA;
- High-risk systems that have the potential to affect the health, safety or fundamental rights of natural persons;
- "Limited risk" systems that require transparency for users, and information where content is generated by AI, such as content generators;
- Minimal risk systems that do not pose a threat to users and whose use is not regulated by regulation, e.g. chatbots, spam filters.

A separate category regulated in the AIA are general-purpose models designed to perform a wide range of tasks and not limited to one specific function or application.
In the context of critical infrastructure, the first two categories of AI systems are particularly relevant: prohibited systems and high-risk systems.
The first category includes systems whose use involves unacceptable risks, i.e. they are completely prohibited due to highly unethical or dangerous activities. The prohibition of certain AI practices stems from broader EU efforts to regulate artificial intelligence in a way that minimizes risks and protects citizens from the potential dangers of modern technology.

Prohibited AI systems

Prohibited practices in the area of using AI systems are listed in Article 5 of the act and include:

Deployment of subliminal, manipulative or deceptive techniques	resulting in a distortion of a person's decision-making, in a way that causes them or others significant harm.
Exploiting any of the vulnerabilities of a natural person or a group of persons	due to their age, disability or a specific social or economic situation,
	resulting in a distortion of a person's decision-making, in a way that causes them or others significant harm.
Social scoring	i.e. the classification of natural persons based on their social behavior or personal characteristics,
	if it leads to detrimental or unfavorable treatment.
Profiling of a natural person or assessing their personality traits	in order to assess the risk of committing a criminal offence.
Untargeted scraping of facial images	from the internet or CCTV footage
	and on this basis create or expand facial recognition databases
Inferring emotions of a natural person	in the areas of workplace and education institutions.
Use of biometric categorization systems	that categorize individually natural persons based on their biometric data
	to deduce or infer their race, political opinions, trade union membership, religious or philosophical beliefs, sex life or sexual orientation.
Use of real-time remote biometric identification systems	in publicly accessible spaces for the purposes of law enforcement.

High-risk systems

The second critical infrastructure category regulated by the AI Act is high-risk systems that have the potential to affect the health, safety or fundamental rights of natural persons.
High-risk AI systems are categorized in two ways.
The first group includes those AI systems that are used as a stand-alone product or are a safety component of products covered by specific EU harmonization legislation. This is primarily about equipment whose absolute safety of operation is of particular importance. In the context of critical infrastructure, it includes, for example, machinery, cranes, equipment and protective systems intended for use in potentially explosive atmospheres, radio equipment, pressure equipment, cableway equipment and rail systems, equipment that burns gaseous fuels, medical devices, civil aviation equipment, including unmanned aerial vehicles, wheeled or motorized vehicles.
The second group includes AI systems used in key areas of human existence, listed in Annex III to the regulation. They include critical infrastructure, within which AI systems

intended to be used as safety components in the management and operation of critical digital infrastructure, road traffic, or in the supply of water, gas, heating or electricity are considered to be high-risk.
As an exception, it is accepted to exclude the systems from the category of high-risk AI systems if they do not pose a significant risk of harm to health, safety or fundamental rights. We will be dealing with such an exceptional situation especially when the AI system does not have a significant impact on the outcome of a specific decision-making process carried out either by a human or by automated means.

2.8.13.2 Obligations of operators of critical infrastructure using artificial intelligence systems

While the only obligation of critical infrastructure operators with regard to prohibited practices will be to verify that the artificial intelligence system in use meets the criteria for a prohibited system (according to Article 5 of the AIA) and, possibly, to recall it, in the case of high-risk systems, the catalog of obligations for those using them is broader.

While the greatest share of responsibilities understandably lies with the system provider, the burden of responsibility for the safe operation of high-risk AI systems has also been placed on importers, distributors and deployers. In the case of critical infrastructure, it is the obligations of the last group of entities (as defined in Article 26 of the AIA) that will apply.

Obligations of deployers of high-risk systems:

1. Take appropriate technical and organizational measures to ensure that they use such systems in accordance with the instructions for use accompanying the systems;
2. Assign human oversight of high-risk systems to natural persons who have the necessary competence, training and authority, as well as the necessary support;
3. Ensure that input data is relevant and sufficiently representative for the high-risk AI system;
4. Monitor the operation of the high-risk AI system on the basis of the instructions for use, and, where relevant, inform providers in accordance with Article 72 of the AIA;
5. Immediately inform the provider or distributor and the relevant market surveillance authority of the possibility that the system used in accordance with the instructions presents a risk within the meaning of Article 79 (1), and suspend the use of the system in such a case;
6. Immediately inform the provider and then the importer or distributor and the relevant market surveillance authorities if a serious incident is identified;
7. Keep the logs automatically generated by that high-risk AI system;
8. Inform workers' representatives and the affected workers that they will be subject to the use of the high-risk AI system;

9. Carry out a data protection impact assessment (DPIA), if applicable, in accordance with Article 35 of the GDPR;
10. Entities that make decisions or assist in making decisions related to natural persons inform the natural persons that they are subject to the use of the high-risk AI system;
11. Cooperate with the competent authorities in any action they take in relation to the high-risk AI system in order to implement the AI Regulation.

In conclusion, the introduction of the AI Act will have a significant impact on critical infrastructure operators. First, it will force verification that the artificial intelligence system used meets the criteria of a prohibited or high-risk system. In the first case, it will entail a recall. In turn, identification of a system as a high-risk one will impose additional obligations on operators in the area of ensuring security, transparency and human oversight. Effective monitoring, reporting and data protection mechanisms will need to be implemented, and it will be necessary to ensure that artificial intelligence systems do not operate in a way that could threaten infrastructure stability.

2.18.13.3 Positive impact of AI on critical infrastructure

Artificial intelligence is playing an increasingly important role in the protection and management of critical infrastructure, which includes resources and systems essential to the functioning of the state and the economy. AI-based solutions are displacing traditional security methods due to their increased efficiency, faster response and adaptability to a dynamically changing threat landscape. Analyzing massive amounts of data in real time, automating security processes, optimizing resource consumption and increasing the effectiveness of response to potential threats are some of the advantages of using artificial intelligence in critical infrastructure. Given the growing security challenges, AI is emerging as an important tool to strengthen the resilience of critical systems and ensure their stable operation.

Prediction and prevention of failures

One possible application of AI in critical infrastructure is **predicting and preventing failures**, thanks to its ability to analyze large data sets. Machine learning algorithms, using historical data and current information from monitoring systems, can detect irregularities before they become noticeable.

Ai-based predictive maintenance makes it possible to **predict equipment failure using advanced algorithms and machine learning**, allowing for intervention before a failure occurs. This technology is used, for example, in the energy sector, where AI analyzes voltage changes in power grids to detect overloads and reduce the risk of failure.

Cybersecurity

The increasing digitization of critical infrastructure is associated with **increased threats of cyber attacks**, which in turn requires a greater focus on digital security. AI systems can significantly increase the level of protection against attacks by using real-time analysis of network traffic, **identifying anomalies and offering advanced tools for proactive detection and prevention of attacks**. AI-based systems dynamically adapt to the evolving threat landscape, recognizing both known and new types of attacks, while optimizing and automating countermeasures.

Some of the most common cyber threats today include phishing attacks. Their effective detection is one of the many areas where artificial intelligence supports critical infrastructure protection. AI plays a key role in detecting and neutralizing such threats by **analyzing message content, identifying anomalies in communications, and monitoring unusual user behavior**. The use of natural language processing (NLP) algorithms allows for effective recognition of messages generated by cybercriminals, which minimizes the risk of breaches and limits the potential impact of incidents. Automated phishing detection processes contribute to protecting sensitive data and ensuring the integrity of critical systems, which is important for the stability and continuity of critical infrastructure operations.

Increasing operational efficiency – automation

Another important area where AI contributes to the development of critical infrastructure is **optimization of operational processes**. AI-based systems enable automation of routine tasks, which translates into increased productivity and savings of time and resources.

Automation eliminates the need for employees to perform repetitive activities, which not only speeds up the completion of tasks, but also minimizes the risk of human error. AI also enables real-time data analysis, which allows for faster decision-making and response to changing operational conditions.

The use of AI in the processes of managing access to critical infrastructure facilities makes it possible to accurately manage permissions, while facial recognition and behavior analysis systems significantly increase the level of security.

An example of the use of artificial intelligence systems can be found in the energy sector, where AI optimizes the operation of nodes by analyzing real-time data and adjusting the energy balance based on forecasts of weather conditions, energy price volatility and the demand for renewable energy sources, heat and gas.

Crisis management support

Artificial intelligence also plays a vital role in supporting crisis management. With the increasing number and complexity of crisis events, AI is becoming an invaluable tool to automate many processes and speed up the response.

AI systems can identify threats and inform relevant services of the need to intervene, which minimizes the risk of human error and increases the efficiency of response to emerging crises. By analyzing large data sets, AI supports the optimization of resource allocation, enabling more efficient use of resources.

Artificial intelligence is also **used in the modeling and simulation of risk scenarios**, making it possible to predict the potential effects of emergency situations and recommend optimal actions. Automating the flow of information between different entities in real time allows faster coordination of activities and more accurate decision-making.

2.18.13.4 Risks associated with the use of AI in critical infrastructure

While the implementation of AI-based solutions in critical infrastructure units can help optimize many processes, it is important to be aware of the risks involved.

Cyber attacks on artificial intelligence systems

Artificial intelligence-based systems, like other ICT systems, can become targets of hacking attacks. At the same time, the peculiarities of the design and operation of AI systems make them susceptible to certain specific types of breaches, particularly those involving data interference and learning processes.

One type of attack specific to AI systems is the **data poisoning attack**. It involves surreptitiously inserting false or manipulated data into the set on which the AI model is trained. As a result, it learns from incorrect information, which will then translate into its incorrect or ineffective operation.

In the process of training an artificial intelligence system, the **backdoor attack** technique can also be used. It involves interfering with the system's learning by inserting hidden functionality or access points (known as backdoors), the purpose of which is to give the attacker the ability to manipulate the system's behavior. The infected AI system will continue to operate normally until a "stimulus" activating the backdoor occurs (e.g., a certain type of input data is fed into the system). This type of attack is very difficult to detect, as the system may not show any anomalies in operation until specific circumstances occur.

Another type of threat is **adversarial attacks**. In this type of attack, subtle changes are made to the input data on which the AI system operates. The purpose is to cause it to make wrong decisions or generate incorrect results. Changes in the data are usually minor and not easily detectable by humans, but they can significantly disrupt the operation of an artificial intelligence system.

In addition to the artificial intelligence system itself, the information contained in its input or training data can also be an attractive target for attackers. To obtain it, they can attempt **model inversion**. To do this, attackers analyze how the AI system operates on

the data and try to invert this mechanism to extract information about the data from the system.

AI-based systems are also vulnerable to "traditional" methods of attack, such as **infection with malware** (e.g., virus, ransomware, etc.), which are most often aimed at disrupting their operation or taking control of them. These types of breaches also make it possible to steal data, access other connected ICT systems, or force the attacked organization to take certain actions (e.g. pay a ransom). They can also be used as a prelude to one of the AI system or data attacks described above.

Other types of risks

Cyber attacks are not the only risks to consider when it comes to using artificial intelligence systems in critical infrastructure. This is because a large part of the risks are related to the nature of AI systems themselves, their limitations and the mistakes their developers and users can make at various stages of the system's life cycle.

Part of this type of risk stems from the difficulty of **effective oversight of AI systems**. Many of them, especially those based on deep learning, rely on highly complex algorithms that even their creators can find challenging to fully understand. For this reason, the AI system may operate in an **opaque manner, as a so-called black box**.

In such cases, oversight of whether the AI system is operating properly and correctly performing the tasks assigned to it can be much more difficult. This entails the risk of **the system making errors** that may **not be recognized by the operator early enough**. The opacity also makes it difficult to trace the various stages of AI system decision-making and audit AI-assisted processes. As a result, such difficulties in oversight can translate into **delayed detection of irregularities**, which in turn poses the risk of even minor faults turning into major failures.

Another problematic issue is ensuring AI systems have the right quality of training and input data. **If incomplete, distorted or false data is entered into the system, it will result in irregularities in the results of the system**. At the same time, such errors can be difficult for a human to detect if they result, for example, in the system working with bias in individual cases, which represent a small percentage of all results. In such situations, AI system malfunctions may not be noticed until their effects accumulate and lead to serious consequences.

Another important risk to consider is the **limited flexibility of AI systems under unusual conditions**. It may happen that during the training of a given system, it has not been provided with data that would teach it to react in very rare, extreme situations (e.g. unusual weather conditions). As a result, such an AI system may not be able to adapt to the circumstances and may react inadequately to them, even making the situation worse.

At this point, it is worth noting another aspect related to the use of AI systems in organizations, namely the phenomenon of **technological dependence**. It can take place in two dimensions.

The first is the **dependence of the organization (or its components) on single technology solution suppliers** (known as *vendor lock-in*). In the case of AI systems, this risk often increases because, given the time and financial resources required to develop them, many organizations rely on off-the-shelf solutions provided by several large players. This can limit an organization's ability to use at least some of its systems from another provider or to optimize them on its own, and in the long run permanently bind it to a particular provider, even if the terms of cooperation deteriorate.

The second dimension is **dependence on the AI system to ensure business continuity**. Such a situation can occur when AI systems are used by an organization in key processes related to the operation of critical infrastructure, while at the same time the operators have not provided adequate procedures in case of failure of these systems. This will be particularly dangerous if there is insufficient oversight of AI systems, which is related to the aforementioned lack of full understanding of their operation.

2.18.13.5 The dangers of using AI in cyber attacks

Critical infrastructure is particularly vulnerable to cyber attacks due to its strategic importance, high dependence on complex ICT systems, and the potentially far-reaching effects of disruption to its operations. Attacks targeting these systems can destabilize the economy, disrupt essential public services or even threaten national security, making it a priority target for cybercriminals.

The most commonly observed types of cyber threats include the following categories:

1. **Ransomware attacks** – involve encrypting key critical infrastructure assets in order to extort a ransom to unlock them.
2. **Supply chain attacks** – involve the compromise of service and software provider systems, leading to secondary infiltration of CI systems.
3. **Distributed Denial of Service (DDoS)** attacks – aim to overload system resources by generating artificial network traffic, resulting in the unavailability of key services.
4. **Attacks on industrial control systems (ICS/SCADA) and operational technology (OT)** – focus on disrupting control processes in sectors such as energy, transportation and water supply.
5. **Social engineering and phishing attacks** – use psychological manipulation mechanisms to gain access to CI systems, most often by obtaining user credentials or infecting end devices.

6. **Wiper attacks** – are characterized by the intentional destruction of data stored in critical infrastructure systems, leading to irreparable operational and financial losses.
7. **Man-in-the-middle (MitM) attacks** – allow interception and modification of data transmitted over communication networks, which can lead to sabotage of operational processes and theft of sensitive information.
8. **Exploitation of zero-day vulnerabilities** – involves exploiting unpatched vulnerabilities in critical infrastructure software before they are identified and secured by manufacturers.

The use of artificial intelligence for cyber attacks not only increases their effectiveness, but also leads to the development of entirely new offensive techniques. The dynamics of this threat means that CI management organizations must identify areas particularly vulnerable to AI abuse on an ongoing basis. Artificial intelligence can be used in particular in several key areas, such as:

- social engineering attacks and information warfare,
- automation of cyber attacks,
- interference with industrial control systems (ICS/SCADA),
- compromising supply chains.

AI in social engineering attacks and information warfare

The use of AI in social engineering attacks can occur primarily on two levels – the creation of phishing or spearphishing message content, and the creation of malware code.

Advanced generative algorithms allow **automatically create more and varied messages** to intensify malicious social engineering attacks and target a wider range of actors. In addition, the use of AI in translating the content of emails enables them to be precisely tailored to the language and cultural context of the intended target, which increases the credibility of phishing attacks and the effectiveness of manipulation campaigns.

The **use of artificial intelligence to automatically generate malicious code** also poses a significant threat, especially to entities with a low level of cybersecurity maturity. AI can be used to create malware based on existing frameworks and models. For example, cybercriminals can, relying on the MITRE ATT&CK framework, generate code with precisely defined properties tailored to attack specific sectors, devices, services or systems – including critical infrastructure.

This approach significantly increases the risk of successful attacks, while escalating the potential consequences of incidents. Moreover, traditional methods of malware detection, based on signatures and heuristic analysis, may prove ineffective against dynamically generated code that has no previous analogs in databases of known threats.

As a result, organizations need to implement more sophisticated detection mechanisms, including behavioral analysis techniques and adaptive threat detection systems, to counter new AI-enabled attack vectors.

Automation and outsourcing of cyber attacks

Automation and outsourcing of cyber attacks should primarily be understood as **using a specific "cyber-criminal services" model, e.g., cybercrime-as-a-service** (CaaS) or its type – ransomware-as-a-service. This makes it possible for a person with no training or experience in preparing malware code to carry out an attack, as long as they have the necessary financial means and basic access to platforms where such services can be purchased.

With AI, cybercriminals can offer advanced tools and services that are readily available on online platforms, often on the deep web or dark web. Artificial intelligence enables **automation and customization of attacks**, making them more effective and harder to detect. One dimension of the CaaS model is the use of encryption software (ransomware) offered by professional "malware providers." This is a particularly serious threat to business continuity for critical infrastructure. The effects of ransomware attacks which successfully encrypt data, systems or devices can pose serious organizational, technical and operational challenges, including the need to restore systems and data and technical infrastructure, as well as to prevent or neutralize the effects of data leakage (the disclosure of data or the threat of doing so has been an essential element of ransomware attacks for some time), including in the communications dimension.

AI in attacks on industrial control systems and technological or production process monitoring systems (ICS/SCADA)

Industrial control systems (ICS) and technological or production process monitoring systems (SCADA) are a special category of vulnerable resources, due to their key role in sectors considered strategic, including in critical infrastructure.

Currently, one of the approaches to ICS/SCADA protection that is widely used and recognized as effective is the use of artificial intelligence and machine learning (AI/ML) based solutions for threat detection. Nevertheless, in the long term, it is expected that the development of AI will lead to the increasing use of AI-generated malware by cybercriminals, as well as sophisticated phishing campaigns targeting critical infrastructure and its users.

In addition, AI can be used to identify and bypass defense mechanisms, making defensive actions significantly more difficult and reducing an organization's overall cyber resilience. The ability to automatically analyze security systems allows for more targeted preparation of cyber attacks and more effective offensive operations. In addition, artificial intelligence can support the process of acquiring and analyzing information on potential attack targets, enabling better profiling of victims and selection

of optimal attack methods. Consequently, the use of artificial intelligence in offensive operations may lead to a further escalation of threats to critical infrastructure and necessitates the implementation of more advanced defense strategies.

Supply chain attacks

In the context of critical infrastructure, **supply chain attacks are of particular importance because they represent a systematic threat, the consequences of which can be difficult to predict and control**. Unlike direct attacks on infrastructure, which often require significant resources and advanced technical capabilities, supply chain attacks allow systems to be compromised while still in the design, production or integration stages. This type of activity allows cybercriminals to gain long-term access to key resources while making their presence difficult to detect.

Critical infrastructure relies on a complex ecosystem of dependencies between hardware, software and service providers. The high degree of interdependence means that **compromising one entity in the supply chain can have a cascading effect, leading to major disruptions across various sectors of the economy and government**, affecting state security, economic stability and the provision of basic services. Sectors such as energy, telecommunications, transportation, healthcare, finance and public administration depend on third-party suppliers to provide both physical and digital infrastructure. As a result, attackers can launch indirect attacks by infiltrating less secure third parties, which then become the infection vector for targeted critical infrastructure systems.

Moreover, one of the most dangerous aspects of supply chain attacks is their **persistence and wide reach**. Unlike traditional cyber attacks, which can be detected and neutralized in a relatively short period of time, supply chain attacks often go unnoticed for long periods of time as malware or modified components become integrated into official production and deployment processes.

2.18.13.6 Recommendations, conclusions, best practices

It is recommended that critical infrastructure operators implement a range of organizational, technical and procedural measures to ensure compliance and minimize the risks of Ai-related cyber threats and vulnerabilities in the supply chain.

Based on the analysis of the impact of artificial intelligence on critical infrastructure, the following recommendations are proposed:

1. **Evaluate the compliance of AI systems used in critical infrastructure entities for their classification under the AI Act**, and then adapt to regulatory requirements. The development of a policy for the implementation, use and updating of AI systems, which ensures compatibility with EU and national regulations, will also be important in this area.

2. **Ensure compliance with national and EU regulations regarding artificial intelligence**, including the implementation of procedures that enable a quick response to legislative changes and the adjustment of organizational policies to new requirements.
3. **Implement a regular, cyclical risk assessment of AI systems used in the organization.** Existing frameworks for risk management and management of artificial intelligence systems, e.g. ISO 31000, ISO 42001, ISO/IEC 23894, will help. Particular attention should be paid to areas such as:
    - AI system's impact on the security, stability and resilience of critical infrastructure,
    - adequacy of mechanisms for monitoring and human oversight of system operations,
    - potential vulnerabilities to adversarial attacks, data poisoning and other manipulations,
    - assessing the quality of training and input data to avoid errors in the performance of AI systems.
4. **Implement a business continuity strategy, including:**
    - developing plans for responding to AI incidents and procedures for shutting down systems when a significant threat is identified;
    - developing and testing emergency procedures in case of failure of AI systems in critical infrastructure;
    - developing plans to reduce dependence on single AI suppliers (minimizing the *vendor lock-in* effect);
    - preparing procedures for restoring data and systems after an AI-driven malware or ransomware attack.
5. **Strengthen human oversight of AI systems, including:**
    - developing and implementing mechanisms to control the results generated by AI;
    - creating internal procedures for monitoring the performance of AI systems in accordance with the operations manual and reporting irregularities to suppliers and regulators.
6. **Ensure the cyber security and protection of AI systems used in the organization, by:**
    - implementation of advanced threat detection mechanisms in AI systems;
    - source code monitoring and software updates – the need for regular AI code audits to identify potential backdoors and hidden vulnerabilities.
7. **Ensure security in the supply chain, including:**
    - risk assessment of the supply chain to ensure that suppliers of AI systems used in critical infrastructure meet the highest cyber security standards, as well as the requirement for transparency and reporting of potential threats

- introduction of stringent requirements for cyber security of AI components, transparency of algorithms, or compliance with EU data protection standards.

8. **Ensure transparency and data protection, including:**
    - ensuring that users and employees at critical infrastructure facilities are informed about the use of high-risk AI and its potential impact on decision-making processes;
    - data protection impact assessments of the use of AI systems.
9. **Include AI risks in the organization's systematic risk assessment.** This should include both the risks arising from the use of AI systems in an entity and the risks associated with using AI tools to conduct attacks against CI.
10. **Cooperation with AI regulators and supervisory authorities, including, for example:**
    - working with national AI supervisory authorities on the implementation of new regulations and AI incident reporting;
    - participation in AI threat information sharing programs at the national and EU levels, such as ENISA.

2.9. Ensuring legal security

Ensuring legal security is a set of measures aimed at minimizing the risks associated with the activities of natural persons or other business entities (state or private) whose actions may lead to disruption of CI facilities, equipment, installations and services.

In ensuring legal security, we are primarily referring to the tools used by the state to secure key CI facilities against hazards. This means the use of legal tools that do not allow, through the ability to control and possibly block or limit the decisions of boards of directors, for example, hostile takeovers, mergers or the sale of certain components of the infrastructure, which could result in disruptions in its operation.

Such tools are provided by the Act of March 18, 2010 on special powers of the minister competent for energy-related matters and their execution in certain joint-stock companies or capital groups operating in the electricity, crude oil and gas fuels sectors (Journal of Laws of 2020, item 2173).

Ensuring legal security within the meaning of the *Act on special powers...* applies only to entities whose property is listed in the unified list of CI in the energy, energy resources and fuel supply system.

Regardless of the solutions adopted by the state, all legal measures should be taken to minimize the risk of disrupting CI. Securing title to the property on which the CI is located, allowing enforcement of access to the CI and securing themselves with agreements with utility providers are examples of good practice in this regard.

2.9.1. Recommendations for agreements with external parties

(1) The CI operator should implement a process for continuously assessing the legal risks arising from its agreements with suppliers of key services and products.

(2) In situations where CI operators use templates issued by the General Public Prosecutor's Office of the Republic of Poland, its recommendations available at www.gov.pl [82] or resulting from direct cooperation can be used.

(3) When selecting a service provider, the current financial and economic situation of the provider should be taken into account, and the ownership structure should be examined, including the identification of beneficial owners.

(1) [82] https://www.gov.pl/web/prokuratoria/rekomendacje-i-wzory-postanowien-umow2

(4) Any relationship with a new partner should begin with a confidentiality agreement. Such an agreement should guarantee real sanctions in case of its violation.

(5) Special attention should be given to relationships with suppliers of IT solutions or products containing computer software that may affect CI's operational capacity, including especially OT systems (e.g. SCADA/DCS).

(6) Any agreement entered into should be subjected to a risk analysis for so-called vendor lock (VL), i.e. dependence on a single supplier. VL is usually associated with unfavorable intellectual property provisions regarding the ability to develop or use products (most often software) in the event of supplier bankruptcy or supplier breakup. The solution recommended for key, "tailored" IT systems is to transfer copyright to the extent that the software can be modified, or to provide a long-term license that allows independent development of the software, including the ability to entrust it to third parties. At the very least, the use of "escrow"[83] mechanisms to source code and the development environment of a given application should be considered.

(7) The target agreement should contain a precise description of the subject of the agreement so as to minimize the risk of areas not clearly assigned to one of the parties.

(8) The agreement should include a description of the expected scope of cooperation of the service provider, including third parties acting on its behalf, co-participating in the provision of the service with the CI operator in a failure removal situation. The scope should include, but not be limited to: the provision of specific infrastructure, personnel and the readiness of such personnel to operate.

(9) Definitions of failures or errors used in agreements should take into account phenomena resulting from the discovery of new software vulnerabilities.

(10) The agreement should include rules for fixing reported errors, in the form of a so-called Service Level Agreement (SLA) containing indicators for cooperation procedures, timeliness of fixing reported errors as well as sanctions for failure to fix them.

(11) Service agreements with software developers should include additional SLAs for remediation of detected vulnerabilities, the exploitation of which may pose a risk of disrupting CI.

[83] Access through escrow to codes – securing the interests of a company by entrusting a third party with the source codes of a particular IT solution. In the event of bankruptcy of a software provider, the third party transfers the source code to the company.

(12) Depending on the identified materiality of the software's impact on CI's operation, it is advisable to regulate access to the source code to the CI operator or an auditor selected by the parties, both during and after the term of the agreement.

(13) The agreement for the supply or maintenance of software should include provisions on the procedure for managing changes to the software and how the service provider's compensation for this should be determined.

(14) The agreement must include sanction mechanisms, granting the CI operator financial (e.g. deductions, contractual penalties) or organizational (e.g. termination of the agreement) rights in the event of a breach of obligations by the supplier.

(15) The agreement should not contain provisions that completely exclude the supplier's liability or limit its liability to amounts that do not correspond to the risks associated with providing a product or service that does not meet the terms of the order.

(16) The agreement should have a formalized escalation path for resolving problems arising from the implementation of the agreement, including a procedure for taking immediate action in the event of hazards to CI resulting from attacks on IT infrastructure.

(17) The agreement should include rules for subcontracting specific activities with the requirement to apply equivalent safeguards as those under the main agreement.

- The agreement for the supply of automation systems software should include provisions to increase security against ICT hazards, i.e.: the supplier's obligation to verify that the supplied software has no known security vulnerabilities and to inform the employer of any existing vulnerabilities,
- a declaration that the architecture of the delivered software allows for the remediation of any security vulnerabilities that are discovered during the software life cycle,
- attached list of all components of the supplied software,
- in addition, it is recommended that the agreement be accompanied by declarations from software developers as to their policies for remediating detected security vulnerabilities, policies for informing users of detected security vulnerabilities, and policies for distributing patches.

2.10. Business continuity and recovery plans

Measures taken to ensure physical, technical, personal, ICT or legal security are preventive measures, which, by design, are intended to prevent the risk of a crisis event from materializing. Despite the proper implementation of security programs, it is not possible to 100% eliminate the risks associated with the interruption of business processes. Therefore, a business continuity plan(s) should be developed and implemented.

One way to decide on the shape of the business continuity system is to use existing standards in this area. An example is ISO/IEC 22301 – requirements for a business continuity management system.

A business continuity plan is a comprehensive document (or set of documents) that defines the organization and how to proceed with planned activities in response to a sudden event beyond the organization's control that results in the interruption of business processes. The BCP should include:

- crisis management plan – describing the principles of organization and conduct of the unit that directs and coordinates the activities undertaken in response to a crisis event,
- contingency plans/procedures that focus on the recovery/restoration of processes and resources after a failure,
- recovery plans/procedures for lost resources (DRP – disaster recovery plan).

The preparation of the BCP must be preceded by an analysis aimed at:

- identification of business processes and related resources,
- determination of the impact of the event on the functioning of the organization (BIA – Business Impact Analysis),
- definition of recovery parameters and conditions for activation of the BCP, taking into account the objectives of the organization and available resources,
- determination of the survival strategy (declaration of the organization's course of action in the event of an emergency).

After responding to the incident and ensuring the continuity of key processes, full (normal) functionality of critical infrastructure should be restored as soon as possible. In order to do this in an efficient and cost-cutting manner, appropriate recovery plans should be prepared in advance (these plans can be part of a business continuity plan).

The effects of risks should be assessed at the risk assessment stage. Although it is impossible to predict all incidents and their interactions, plans should be as concise as possible. In small organizations, a single plan covering all actions needed to restore full functionality of critical infrastructure is sufficient. In large organizations, it makes sense to divide the plan into sections, each detailing how facilities, services, equipment, installations will recover from various types of incidents.

It is recommended to divide the plans by resource recovery strategy:

- human (knowledge, skills),
- location (workplaces),
- technological (installations, equipment),
- information (real as well as virtual: agreements, customer registry),
- supply chain, etc.

Potential suppliers of materials, products or services needed for recovery should be identified in advance. If materials, products or services are not available "off-the-shelf" in the market, it is advisable to enter into preliminary agreements to obtain priority for orders. If it is not possible to conclude priority agreements, consideration should be given (if there are technical and economic possibilities) to the storage of materials and products that are key to the restoration of CI owned by the organization. If warranted, verify what funding sources can be used for recovery.

All plans must receive management approval and be available to all employees with responsibilities in the response and management phases of an emergency event, activation and implementation of the business continuity and recovery plan. Authorizations for decisions or expenditures should be clearly documented.

The plan should include hierarchical objectives specifying the areas of restored operations and the expected time after which operations should resume to a specified level. Successive implementation of the objectives will ensure that CI returns to its pre-incident state.

The selection of people responsible for managing each phase of recovery is crucial. They should be people with extensive knowledge of the characteristics of the operation of critical infrastructure, organizationally proficient, who, after being assigned tasks, based on the plans prepared, will develop a long-term policy for the management of emergency operations and the return of CI to its pre-disaster state, while implementing new solutions to ensure an even higher level of security.

When preparing business continuity and recovery plans, the efficiency of the process can be improved by applying the following measures:

- obtaining and storing in a safe place the plans of the CI that needs to be rebuilt after a failure – access to the pre-disaster plans can significantly shorten the recovery process,
- establishing (verifying) rules and deadlines for compensation and insurance for the lost components of CI,
- preparing a strategy for financing the recovery of the rest of CI (not covered by compensation and insurance),
- establishing (verifying) the scope of approvals and permits that will need to be obtained in the event of infrastructure recovery,
- agreeing with other CI operators in terms of planned repairs and other outages of similar CI,
- determining the principles, including frequency, of updating recovery plans,
- periodically testing the business continuity and recovery plans by comparing their content with the organization's investment plans (this comparison is intended to identify other relevant components that are part of the current investment plan and could be added to the recovery plans).

It is good practice to integrate the management systems in place in the organization, including:

- Information Security Management System;
- Business Continuity Management System,
- IT Service Management System;
- Environmental Management System;
- Quality Management System.

2.10.1. Contents of the business continuity plan

The organization should establish documented procedures for responding to a disruptive incident and procedures that address how to continue or restore its operations within the established timeframe. Such procedures should take into account the requirements of those who will use them.

Business continuity plans should collectively include:

(1) Defined roles and responsibilities of individuals and teams with authority during and after an incident;
(2) The process that triggers the reaction;
(3) Details of how to manage the immediate consequences of the incident, with particular attention to:
    a. the welfare of individuals,
    b. strategic, tactical and operational response options,
    c. prevention of further loss or unavailability of priority activities;
(4) Details of how and under what circumstances the organization will contact employees and family members and key stakeholders, as well as details of emergency contacts;
(5) The organization's means of continuing or restoring priority activities within the established timeframe;
(6) Details of the organization's contacts with the media after the incident, including
    a. communication strategy,
    b. preferred platform for communication with the media,
    c. guidelines for or model statement to the media,
    d. relevant spokespersons;
(7) The process of withdrawing the plan if the incident subsides.

Each plan should define:

(1) Intent and scope;
(2) Objectives;
(3) Commissioning criteria and procedures;
(4) Implementation procedures;
(5) Roles, responsibilities and rights;
(6) Communication requirements and procedures;
(7) Internal and external linkages and impacts;
(8) Resource requirements; and
(9) Information flow and documentation processes.

Both business continuity and recovery plans, as well as personal, legal, physical, ICT and technical protection, must be treated equally as key components of security management. Security management also requires interdisciplinary organizational, engineering and humanities knowledge and a focus on managerial and employee competencies in all its core processes and the services that support them. Having knowledge of the risks, their areas of occurrence and their interrelationships and interdependencies, as well as the ability to take preventive action and in the processes of materializing risks, allows all employees and stakeholders to build security responsibly and sustainably.

The purpose of developing, updating and applying any type of plan based on risk management and effective incident response is for the organization to implement mechanisms that strengthen resilience to diagnosed hazards by reducing risks to acceptable levels and preparing for events that may bring unwanted losses.

3. Glossary of abbreviations

No.	Acronym	Explanation
1	*APT*	Advanced Persistent Threat
2	*BCP*	Business Continutity Plan
3	*BIA*	Business Impact Analisys
4	*CCTV*	Closed Circuit TeleVision
5	*CERT*	Computer Emergency Response Team
6	*CSIRT*	Computer Security Incident Response Team
7	*DNS*	Domain Name System
8	*DR*	Disaster Recovery
9	*DRP*	Disaster Recovery Plan
10	*ENISA*	European Network and Information Security Agency
11	*IDS*	Intrusion Detection System
12	*CI*	Critical Infrastructure
13	*IPS*	Intrusion Prevention System
14	*MTBF*	Mean Time Between Failure
15	*MTTF*	Mean Time To Failure
16	*MTTR*	Mean Time To Repairs
17	SotRoCE	Standards on the resilience of critical entities
18	*RBM*	Risk Based Maintenance
19	*RCM*	Reliability Centered Maintenance

No.	Acronym	Explanation
20	*SCADA*	Supervisory Control And Data Acquisition
21	*SIEM*	Security Information and Event Management
22	*ACS*	
23	*SLA*	Service Level Agreement
24	*IAS*	
26	*WAN*	Wide Area Network
27	*VLAN*	Virtual Local Area Network
28	*VPN*	Virtual Private Network
29	*VL*	Vendor Lock
30	*VSS*	Video Surveillance System

List of tables and figures

List of tables

List of figures