Risk Management for the Needs of Critical Infrastructure

A. MACHNACZ
a.machnacz@policja.gov.pl

Police Headquarters
Domaniewska Str. 36/38, 02-672 Warsaw, Poland

The content of the article presents a proposal for implementing the risk management process for the protection of critical infrastructure as an important element in the process of ensuring the national security and its citizens, and the also the smooth functioning of public authorities as well as the public administration with its institutions and entrepreneurs. Various stages of risk management are discussed, including its planning, identification and analysis, and also risk response planning and its monitoring and control. A very important role was indicated in the process of risk management to ensure the security of critical infrastructure, including a presented proposal of risk calculation as a method of optimizing security costs.

Keywords: critical infrastructure, risk management, national security.

1. Introduction

The development of civilization and the rapid technological change marked the beginning of the fundamental transformation of the social structure and the way of life of the individual. As a result of technical progress television appeared, digital television, mobile phones, internet, personal computers, which revolutionized life. Increasing automation and the use of machines to perform operations previously carried out by people not only contributed to increased efficiency, but also to human dependence on this type of solutions. The changes enabled the easy and rapid exchange of information between offices, health centres, research institutes and universities, as well as between government institutions, and citizens and businesses. At the same time, it became possible and common to conduct daily activities through the internet, such as: online shopping, scheduling doctor appointments or managing official matters.

By observing the development of civilization it can be concluded that intensive technological change, and what comes after, the development of advanced information technology and automation has increased the quality and comfort, but also contributed to the growth of risks. Now, it would be difficult to function without well operating supply systems: energy, water and food, communications systems and networks, financial and transportation systems, or even rescue and chemical manufacturing systems. The violation of the continuous operation of the public administration might cause destabilization of a functioning of the nation. All these elements affect the security of the state and its citizens, including the effectiveness of authorities and public administrations as well as institutions and entrepreneurs, which are part of the so-called critical infrastructure [1], whose protection should be one of the main priorities of each country [2].

The development of technology puts the public authorities and other institutions under threats that could lead to a breach of the integrity and continuity of critical infrastructure. The development of mass media and the internet guaranteed flow of information that has become simultaneously a great tool in the hands of terrorist organizations allowing them to gain significant public and media effects by shaping the behaviour of the authorities and thus obtain the expected results in the destruction or disruption of critical infrastructure. Analogous consequences can result not only from intentional and unintentional human activities, but also may be the result of the forces of nature.

In order to counter threats of destruction, damage or disruption of the critical infrastructure, it becomes important to take coordinated actions by all entities in the area of protection of this infrastructure. One of these actions is the current performance of risk analysis and converting its results to the implementation of security measures. These actions are directly related to risk management, which consists of constant monitoring of the elements of this infrastructure and reducing the potential for adverse events by estimating values, the so-called risk factor relating, referring to the status of systems and including related operating facilities, equipment, installation and key services for the safety of the nation and its citizens [3], [7]. This overall

process of identifying, controlling and eliminating or minimizing the likelihood of events that may affect critical infrastructure resources, requires a disciplined, consistent and reliable approach. This will ultimately allow avoiding the risk, taking preventive action or transferring the risk or its diversification. These activities are basic strategies to counter the risk, under which security measures are chosen.

Fig. 1. Stages of risk management
Source: own work

It is worth noting that risk management is a process consisting of well-defined, successive and mutually determining the stages, creating simultaneously a repeating cycle, as shown in fig. 1, in which the important element is the constant communication of any emerging risks. The effects of the actions taken and developed materials in one phase constitute a data source for the next step in the cycle of risk management. It is important that the selected processes, such as risk identification, take place continuously.

Later in the article, based on the PMBOK methodology [4] a proposition is presented of a risk management system for the protection of critical infrastructure allowing the current identification of risks, determining their size and identifying areas needing safeguards.

2. Planning Risk Management

Effective risk management, irrespective of the form and area of operation, first of all requires planning that consists of predicting how will various processes or events be developed in the future, as well as for programming and developing a plan.

Planning risk management for critical infrastructure protection should rely on the preparation and organization of the risk management process, under which will be determined, among other things: the thresholds of risk acceptance, the system of evaluation and interpretation of events, early warning indicators, and also the creation of the organizational structure. The task of such a structure should be to take action for the isolation, reduction and eventual elimination of these risks, as well as alternative methods of preparation, in order to protect against threats, which may occur during the planning and execution of works relating to the protection of critical infrastructure.

The result of the work undertaken within the framework of planning for the security of the critical infrastructure should be the creation of the so-called risk management plan containing [5]:

1. A general description of actions, as the basic presentation of all works, for which applied risk management will be used, including suggestions when and how risk management should be applied.
2. Description of the roles and responsibilities associated with them, as a list of duties and permissions of risk management for individual owners of elements of the critical infrastructure, including rules for reporting and issues escalation paths.
3. Description of the risk management process, as a representation of each of its steps, and an indication of when each of them will be used along with the eventual determination of any deviations in this area and the reasons for such deviations have been made, including subjecting the process characteristics to continuous tracking of risk.
4. Indicating categories, indicators, evaluation system and risk acceptance thresholds, including:
   - categories of risks and responses to risk depending on whether it is perceived as a threat or as an opportunity
   - indicators for early warning, i.e. risk materialization, by measuring changes in the critical areas regarding the functioning of critical infrastructure and to identify appropriate preventive actions as well as defining conditions and a time of their launch
   - ratings system, as a method of visualization of risks, which is used in risk analysis and for the interpretation of obtained results
   - thresholds for risk tolerance and acceptance thresholds, that is criteria for determining when actions should be taken in response to the identified risks.
5. Estimate the budget required to ensure efficient risk management.

6. Description of tools and techniques supporting the risk management process, including data sources that can be used.
7. Determining documentation requirements, including:
   - how to create documentation of the risk management process, including a description of the reporting system as a statement of purpose and destination, frequency, structure and required contents of reports
   - available document templates, their purpose and location, in order to achieve consistent reporting and the possibility of aggregation of information from individual reports, including the preparation of templates, including a risk response plan and risk register
   - principles of assuring control and quality of documents, their versions, how to store, uniform structure and format, mode of applying corrections, consistency between the documents as well as approval, review and feedback.
8. Description of the method of periodic review of the risk management plan as a way to verify the risk management practices, including checklists tailored to the type of activities and a list of issues requiring attention, including supplementary information sources.
9. The schedule of activities related to risk management.
10. Glossary of terms as an element allowing to unequivocally understand the various issues contained in the plan by all participating entities.

Included in the risk management plan the description of the actions and roles, as well as responsibilities, should present the main tasks of the critical infrastructure security area and the corresponding targets with specific timeframes, as well as identifying those entities responsible for their achievement. Moreover, the description should make demands on the process of circulation and approval of all documents created within the framework of risk management to prevent the omission of relevant entities, whose potential comments and suggestions could substantially affect the minimization of risk. Presenting the different steps of the risk management process used and specifying the conditions of their implementation should allow the visualization of the logical consistency of the entire approach to the management process for the sake of completeness and correctness of all operations. Bypassing any of the described steps could lead to omission of some factors that decide the target model of critical infrastructure security.

By considering the critical infrastructure certain categories of risk can be distinguished covering areas such as: technical, organizational, external and environmental. In each of these areas both risk and individual risk factors can be isolated. Such a division allows to organize the types of risks due to the source origin, and thus makes it possible to dedicate specialized resources for each category. The technical area may include all of these risks, which relate to the broader meaning of technology, including support automation solutions that are modern elements of critical infrastructure. The adopted structure of management and coordinating activities under the security of this infrastructure will form another category of risks. The group of external threats will be the factors arising from natural causes or from human activity, including terrorism, which may cause adverse changes in physical, chemical or biological resources, creations and constituents of the protected wildlife. To the last above-mentioned category, i.e. the group of environmental risks, can include risks arising from natural disasters, including: floods, fires and earthquakes.

To ensure the proper and orderly process of dealing with risks in the area of critical infrastructure security, the following response categories to risk can be specified [5]:

1. REDUCTION – take action to reduce the likelihood of the occurrence or minimize the effects, if the threat were to materialize.
2. ELIMINATION – changing the selected element associated with the operation or infrastructure security, such as: changing the management organization, technology, suppliers, production method, etc.
3. TRANSITION – transferring responsibility for specific risks to a third party, such as by purchasing insurance.
4. ACCEPTATION – a conscious decision to refrain from any combination of preventive and simultaneous constant monitoring of a given risk in terms of assessing whether they should still be tolerated.
5. SHARING – some form of risk sharing between parties according to established rules.

The risk management plan, cannot forget about the early warning indicators, the ratings system in terms of the interpretation of results and thresholds of tolerance and risk acceptance, which appropriate definition is the essence of all actions to secure critical infrastructure often

crucial for an appropriate response to emerging events.

However, it is important to estimate the budget relating to risk management. Keep in mind that in practice often possessed financial resources affect the selection of protection mechanisms reducing identified risks, but also their absence or excessive limitation makes it impossible to implement all required safeguards. The risk management plan should also include a description of the specialized tools and proven techniques, which without their support would make it difficult to efficiently conduct, for example, a risk analysis or an appropriate risk response plan for such a huge list of resources that the critical infrastructure and threats associated with it creates. Examples of techniques, which can be used in various stages of risk management, as well as tools to perform procedures and fast calculations supporting these techniques may be classified as follows [5], [6]:

- TECHNIQUES: BPEST (Business, Political, Economic, Social, Technological) analysis, PESTLE (Political Economic Social Technical Legal Environmental), FMEA (Failure Mode & Effect Analysis) and CRAMM (CCTA Risk Analysis and Management Method)
- TECHNIQUES: Event tree analysis and fault tree analysis
- TECHNIQUES: Dependency modelling and real option modelling, and also decision-making in conditions of risk and uncertainty
- TOOLS: PEST Advanced Software Analysis Tool, SWOT Expert, CRAMM Expert, RISKAN, Deep SWOT analysis software, PILAR / EAR.

In addition to the above-mentioned techniques also used are questionnaires, prospecting, business studies and scenario analysis, industry benchmarking, risk assessment workshops or hazard & operability studies. The are many supporting software for these techniques, both commercial and open-source, such as SmartDraw or EBIOS.

Ensuring adequate quality of work requires the formulation of requirements for the created documents through the preparation of document templates. They allow repeated consistency assurance of the created documentation and to speed up work, especially if it is required, just as it is in the case of critical infrastructure, aggregating data from different entities. Described in the risk management plan, the monitoring and verification methods are to make the entire process practical and ensure its continuing topicality, consistency, completeness and consistency of requirements contained therein. The lack of control procedures and periodic review of the risk management plan could bring comparably irreversible effects, than the lack of the same plan. To ensure the preservation of the time regime of carried out tasks in various phases in the risk management plan the schedule of actions is defined showing the various stages and the expected results on the timeline maintaining the infinite cycle. Planning the course of activities in time helps to raise awareness of the scope as well as the relationship between them, it makes easier to supervise and the early detection of implementation threats. The richness of language causes that the placement of an adopted nomenclature into the risk management plan often allows for the exclusion of contradictions and confusion as to the importance of specific issues.

A high quality product in the form of a risk management plan translates directly into successive stages of management. It provides the mechanisms necessary to analyze and identify risk reduction measures, as well as it systematizes and organizes the approach to the entire process to ensure its completeness and consistency.

All work associated with creating and updating a risk management plan for critical infrastructure security, due to its nature and contents, should be subject to laws on the protection of classified information.

3. Risk Identification

Another action in the cycle of risk management is that its identification is reduced to detecting sources of risk and its description, and then systematizing risks according to accepted categories. Due to the nature of the steps the process should be performed several times during both the planning and in the endless cycle of risk management.

The description of risk is its term by giving its source, event (incident or accident), causing the risk and the reasons allowing the emergence of risk as well as what effects this risk calls. The event is the occurrence of or the change in specific circumstances that may occur once or repeatedly.

The process of identifying risks for the needs of critical infrastructure security should be an iterative process, carried out in all phases and stages of risk management. It should involve all entities, which are ruled by different

infrastructure resources, including its complex nature and any functional dependence between its elements. It is appropriate to provide the information base and personally involve people with appropriate knowledge of the area.

Defined in an earlier phase of risk categories allow to qualify all unfavourable events that may occur during the planning and implementation of the continuous risk management process, and thus constitute a unified mechanism for collecting and processing such information.

The main result of the risk identification stage is a list of identified sources of risk in the area of critical infrastructure security. This list should also include a list of activities that trigger, i.e. symptoms and warning signals, indicating the circumstances of the occurrence of adverse events. The structure of the list of risk sources for the needs of critical infrastructure security could take the following form:

- risk identification, facilitating its monitoring and control
- category, cause and nature of the risks, which includes the given factor (risk, opportunity)
- the name or description of all or part of the critical infrastructure, which the risk concerns, including giving entity names in which the properties are specific elements of the infrastructure
- the effect of risk in the form of the description of the effect of the occurrence of a threat or opportunity
- risk symptoms as circumstances indicating that there has been or there will soon be a to risk occurrence.

It is important at this stage that no risks be ignored, whose sources are beyond the control of the authority responsible for critical infrastructure security. We should not neglect the study of individual results of side effects and identify possible causes and scenarios showing what effects may occur.

Implementation of the risk identification process is supported by techniques and tools identified in the planning stage of risk management. Predicting what events may significantly affect the non-fulfilment of planned tasks would be much harder without the possibility of using these techniques and specialized tools.

The proper execution of this stage is only possible if you have a good knowledge of the critical infrastructure, as well as an excellent knowledge of all related matters, including the environment in which it operates. Underestimating or omission of any of the risks would cover only a fragment of reality, which would affect the nature and meaning of risk management.

4. Qualitative and Quantitative Risk Analysis

Another element of the whole process of risk management is its analysis phase, during which the estimated size of the probability and consequences of the existence of previously identified risks. It is a process for understanding risk and to determine its level. Gathered here are the basis for risk assessment and decision-making in dealing with it. The results of this phase are the basis for further planning for adverse occurrences.

Carrying out risk analysis for the needs of critical infrastructure should begin in the so-called qualitative analysis consisting of putting identified risks in a hierarchy according to their potential impact on infrastructure security, including the possible distance in time. This operation should be based on the filtration of these risks, in order to determine, which of them can be accepted because of the minima probability of the occurrence and which and in what order should they be subject to further analysis and risk response plan. As a result of the qualitative analysis an approximate assessment of the risk factor probability and an estimate of risk significance or circumstances identified as a risk factor should be obtained. Repeating this type of analysis and testing obtained results will naturally allow the observation of trends that may constitute a legitimate basis for the decision to intensify or reduce operations involving risk management.

The result of the implementation of quality risk analysis for critical infrastructure security should be a list of risks in terms of priorities in planning and taking preventive actions as well as a list of risks for further analysis.

For the case of identifying risks of significant impact on critical infrastructure security the quality analysis should be supplemented with a quantitative analysis, involving the definition of measurable probability size values as well as the consequences of adverse events. Such a measurement can determine the chance of achieving an appropriate security infrastructure, and also determine the necessary reserve levels of time and cost, which may be needed to compensate for the effects of the occurrence of individual risks.

The group of basic tools and techniques used for quality risk analysis include scales and matrixes probability assessments as well as the impact of risk occurrence. For the quantitative analysis, tools are different from each other, because of the degree of complexity and they often include:

- survey research on the occurrence of certain events, in order to determine the probability size and the impact of the occurrence of risk
- simulation techniques for generating hypotheses concerning the probability of an occurrence of a particular scenario of operating conditions and the protection of critical infrastructure
- an analysis of decision trees, which allows to build sequence diagrams with their defined probability and costs, including each possible logical paths of events
- sensitivity analysis allows the determination, which risks have potentially the greatest impact on infrastructure security.

The result of quantitative risk analysis for critical infrastructure security should be:

- list of measured quantified risks in order of priority, which is used to plan and take preventive action
- Probabilistic analysis includes projections of cost and time of implementing tasks for infrastructure security, including the probability size of achieving the objectives of cost and time
- list of trends that characterize the results of quantitative risk analysis obtained on the basis of its execution several times and used for ranking risks in terms of priority in planning and taking preventive action.

Cumulative risk analysis may therefore be a combination of the above dependencies on the in relation to circumstances of the available information, data and resources. The mere presentation of the results of risk analysis can boil down to determining their impact and their probability on the timeline grouped by situation and expressed in a tangible or intangible method.

5. Planning Risk Reaction

Risk analysis has provided material support to make decisions about the priorities of conduct in relation to specific events. By taking definite steps takes into account the wider context of risk. This applies to the circumstances of the impact on authorities that do not bear direct responsibility or benefits with taking risks in relation to the authorities directly responsible for the risk and the outcome of actions resulting from decisions made. This can lead, in particular, to the decision of not proceeding with the risk in any way except for only using control measures on it.

Therefore, the key step in the risk management process is planning a response to risk allowing the indication of variations of proceeding in terms of eliminating the risks and increasing potential benefits. This process shows, based on the defined categories during the planning phase, the response to risk, possible reactions by indicating appropriate actions as well as assigning the responsible entities for carrying out actions related to the risks. Planning a response to the risk for critical infrastructure security should take into account such a plan of proceedings, so that actions taken would be most effective. Planned responses should be proportionate to the effects of adverse events, eliminate (or suppress) the impact of the given threat in a manner that is cost-effective and be implemented on time. This requires the involvement of many institutions, which are in charge of the individual elements of the infrastructure.

The main result of the reaction to risk planning phase for critical infrastructure security should be to prepare the so-called response to the risk plan with a list of residual and secondary risks, i.e. such that remain even after the implementation of strategies to reduce, eliminate, transfer, accept or even risk sharing. Risk response plan should take into account the results of qualitative and quantitative analysis of risks and the arrangements for their administrators, along with a description of actions that constitute a response to the risk. For each action a duration and financial resources should be specified, including other resources required to implement them. In case of risk acceptance contingency plans should be defined.

Planning response to risk is reduced to developing a plan for dealing with risk, which should include:

- choosing what kind of impact to have on risk
- selecting the mode of implementation of the given method, including the selection or modification of control measures
- prepare and implement a plan for dealing with risk.

Selection of how to impact on risk is a cyclical process and includes:

- conduct a risk assessment
- determine a tolerable level of risk

- assess the effectiveness of a given course of action.

Selecting the mode of implementation of a given course of action is reduced to the analysis of cost and effort necessary to implement the given mode in relation to the benefits. It is very important that each of the analyzed modes take into account legal requirements and other regulations including social responsibility and the impact on protecting the natural environment. The mere implementation of a given mode should be carried out according to the plan for dealing with risks, in which powers and responsibilities are clearly defined in relation to the given implementation.

The preparation and implementation of a plan for dealing with risk is aimed at documenting how to implement certain modes of conduct. They should include in particular:

- justifying the selection along with the expected benefits
- a list of people and responsibilities
- a list of indicators along with the limit values
- the way of communication and the rules for monitoring
- the required deadlines and schedule.

It is desirable that the plans of conduct be linked with the management processes of the given body responsible for the entire process.

6. Monitoring and Controlling Risk

Preparing adequate actions in the area of preventing critical infrastructure threats requires their implementation, current tracking of their execution and controlling the status of each identified risks.

Monitoring and controlling risk for critical infrastructure security requires maintaining an adequate reporting system by all entities, to whom competencies are specified for elements of infrastructure. This task comes down to constantly checking, whether the identification and evaluation of risk are properly done as well as if appropriate measures and solutions are applied, and also whether unidentified risks have already occurred. Observation of the identified risks, including residual and secondary risks, as well as implementing risk response plans and evaluating their effectiveness can determine whether preventive action taken in response to the risk yield expected results or require reconstruction. This should be a component of the risk management process. The very process of monitoring and control should be characterized by, among others:

- be subject to regular checks and supervision,
- be carried out periodically or ”ad hoc”
- have clearly defined responsibilities and scope
- provide new information for risk assessment
- enable the detection of trends in risk assessment
- document the results and enable reporting.

Components to monitor and control risk are:

- monitoring understood as a continual observation and checking of the status, in order to identify changes of the given parameter
- review understood as an action taken to determine the suitability and effectiveness of a given parameter
- audit understood as an independent and documented process of obtaining an objective assessment of the scope and effectiveness of a given parameter
- reporting understood as a form of communication used to inform entities the of the risk management process about the results of the given parameter or the entire process.

The result of the monitoring and control processes of risks for the needs of critical infrastructure security should be:

- assessment of the introduced measures in terms of their effectiveness
- list of necessary corrective actions necessary to take in case of ascertained errors during the implementation of the establishments resulting from the risk response plans
- proposal of actions related to newly identified risks.

The complexity of the critical infrastructure and the associated risks that are dynamic and operate in a changing environment, make it an important element in the infrastructure security process are the accepted principles of risk management. It is extremely important of carrying out periodic audits of their compliance with common acceptable standards, as well as the ability to introduce improvements.

7. Conclusion

In view of the still emerging threats to critical infrastructure the key issue is risk management. However, without a unified risk management system for such a broad spectrum it would be

impossible to appropriately and effectively plan and implement security measures. Ignoring the risk management planning stage would have unimaginable consequences for the security of critical infrastructure, because the next steps in the identification, analysis and planning a response to risk would completely be deprived of mechanisms for a reliable identification of risks, their assessment and planning countermeasures.

Indication for the entities, who are authorities of the elements of critical infrastructure, preparing, for example, crisis management plans and critical infrastructure security plans of a homogenous risk management system, could contribute to a more effective process of identifying and assessing risks, thus optimizing the cost of building the critical infrastructure security.

An important element of risk management should not only protect critical infrastructure, but also develop such solutions, so that potential damage and disruption in its functioning would be probably short, easy to remove and would not cause additional losses for citizens and the economy. The essence of these tasks should not only come down to protecting critical infrastructure from threats, but also to reduce their effects and its rapid recovery in the event of failure, attacks and other events disrupting the proper functioning of the state and its citizens.

Due to the complexity of critical infrastructure, which proper functioning often depends on many entities and institutions of the public administration are essential formal arrangements with the scope of responsibilities that they take on themselves other participating sides in the security of critical infrastructure and responding to various threats, including the implementation of actions resulting from the contingency plans.

The demand of the necessity of documenting should be emphasized, which causes all activities related to risk management to be identified. All records also provide a basis for improvement (learning) of methods and tools, as well as the entire risk management process.

8. Bibliography

[1] Act of April 26, 2007 on Crisis Management (Journal of Laws 2007 No. 89 pos. 590 with amendments).
[2] A. Tyburska (red.), *Ochrona infrastruktury krytycznej*, WSPol Szczytno, 2010.
[3] ISO 31000:2009, Risk Management – Principles and Guidelines.
[4] *A Guide to the Project Management Body of Knowledge (PMBOK® Guide)* – Fourth Edition, Project Management Institute (Corporate Author).
[5] *Management of Risk: Guidance for Practitioners*: 3rd Edition, M_o_R publication, OGC – Office of Government Commerce (Author), Great Britain, 2010.
[6] *A Risk Management Standard*, Published by AIRMIC, ALARM, The Institute of Risk Management – IRM, 2002.
[7] ISO/IEC 27005, Information technology – Security techniques – Information security risk management.

Zarządzanie ryzykiem na potrzeby infrastruktury krytycznej

A. MACHNACZ

W treści artykułu przedstawiono propozycję realizacji procesu zarządzania ryzykiem na potrzeby ochrony infrastruktury krytycznej jako istotnego elementu w procesie zapewnienia bezpieczeństwa państwa i jego obywateli, a także sprawnego funkcjonowania organów władzy i administracji publicznej oraz instytucji i przedsiębiorców. Omówiono poszczególne etapy zarządzania ryzykiem, w tym jego planowanie, identyfikację i analizę, a także planowanie reakcji na ryzyko i jego monitorowanie oraz kontrolowanie. Wskazano bardzo ważną rolę zarządzania ryzykiem w procesie zapewnienia bezpieczeństwa infrastruktury krytycznej, w tym przedstawiono propozycję kalkulacji ryzyka jako metody optymalizacji kosztów środków ochrony.

Słowa kluczowe: infrastruktura krytyczna, zarządzanie ryzykiem, bezpieczeństwo narodowe.