VÉDELEM TUDOMÁNY
KATASZTRÓFAVÉDELMI ONLINE TUDOMÁNYOS FOLYÓIRAT

Mészáros István

EGÉSZSÉGÜGYI LÉTFONTOSSÁGÚ RENDSZERELEMEK KOMPLEX ÜZEMELTETŐI BIZTONSÁGA, KÜLÖNÖS TEKINTETTEL AZ IPARBIZTONSÁGI FELADATOK ELLÁTÁSÁRA

Absztrakt

Hazánkban 2016-ban kezdődött meg az egészségügyi ágazatban, azon belül is fekvőbeteg-ellátás alágazatban a létfontosságú rendszerelemek azonosítása és kijelölése. A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló törvény, illetve végrehajtási rendelete a kijelölt rendszerelemek üzemeltetői számára Üzemeltetői Biztonsági Terv készítését írják elő. A 2020-ban történt felülvizsgálatok során új típusú tervezési és kockázatértékelési módszertan került kiadásra. Az üzemeltetői biztonsági tervezéshez a nemzetközi gyakorlatban bevált, az üzletmenet-folytonossági menedzsment rendszerek tervezését leíró, ISO 22301 sz. szabvány alkalmazása azonban hazánkban nem jellemző ezen a területen. Az egészségügyi igazgatásban a profitorientált, így a „termelés” és a „profit” fenntartására fókuszáló szemléletmód gyakorlati alkalmazása nem megszokott, a profit és a termelés fogalma nehezen értelmezhető. A tanulmány az üzletmenet-folytonossági menedzsment rendszerek közegészségügyben történő alkalmazási lehetőségeit vizsgálja.

Kulcsszavak: létfontosságú rendszerelem, kritikus infrastruktúra védelem, egészségügy, fekvőbeteg-ellátás, üzemeltetői biztonság, üzletmenet-folytonosság, kockázatértékelés

VÉDELEM TUDOMÁNY
KATASZTRÓFAVÉDELMI ONLINE TUDOMÁNYOS FOLYÓIRAT

COMPLEX OPERATOR SECURITY OF CRITICAL INFRASTRUCTURES IN HEALTHCARE SYSTEM, WITH PARTICULAR REGARD TO THE PERFORMANCE OF INDUSTRIAL SAFETY TASKS

Abstract

In Hungary, the identification and designation of healtcare sector's critical infrastructures began in 2016, including the inpatient care sub-sector. The act on the identification, designation and protection of critical systems and facilities and its implementing decree requires operators of designated system components to prepare an Operator Security Plan. During the revisions in 2020, a new type of planning and risk assessment methodology was issued. ISO 22301, which describes the design of business continuity management systems, has proven itself in international practice for operator security planning. However, the application of the standard is not typical in this area in our country. In health care sector, the practical application of a profit-oriented approach focusing on the maintenance of "production" and "profit" is not common, and the concepts of profit and production are difficult to interpret. The study examines the application possibilities of business continuity management systems in public healthcare sector.

Keywords: critical infrastructure protection, health care sector, in-patient care, operator security, business continuity, Risk Analysis, Business Impact Analisys

1. PROBLEM STATEMENT

In Hungary, the legislation on critical infrastructures entered into force in 2012. This is the Act CLXVI of 2012 on the identification, designation and protection of essetial systems and facilities (Act of CIP). The government decree 65/2013 (III. 8.) on the implementation of the Act CLXVI of 2012 on the identification, designation and protection of essential systems and facilities defines the rules of designation/withdrawal, the tasks of the security liaison officer

and general expectations for its employing, as well as the obligation to prepare the Operator Security Plan (OSP). The basic content of the OSP is defined in Annex No. 2. of the Act was defined by the legislator. In addition, some sectoral legislation may prescribe additional mandatory content elements. The government decree 246/2015 (IX. 8.) on the identification, designation and protection of critical health systems and facilities entered into force in 2016 for the healthcare sector. The decree defines the sub-sectors and designation criteria, the sector-specific rules of the identification procedure and designation, as well as the sector requirements imposed on the security liaison officer.

In the international professional terminology the preparation of the OSP is based on the Business Continuity Planning (BCP) planning practice in the private sector, i.e. a comprehensive approach to business continuity, which is basically a company management, process-based approach. That gives dynamism to the plan and the "maintenance" of the plan. This dynamism is provided by the identification of basic processes and their cyclical management.

Standardized quality management systems are best suited for this type of planning and management tasks. The basics of the business continuity planning and management system are described in the ISO 22301:2020 standard.

In this study, I want to examine and establish the possibilities of introducing the standard into the public health sector, including the in-patient care sub-sector, by integrating the business continuity approach and the first steps of planning into the system.

2. THE CYCLICALITY OF MAINTAINING THE BUSINESS CONTINUITY SYSTEM

Both administration and public administration are based on cyclical processes, which ensure that the properly set goal is achieved by involving the appropriate resources. That ensure that the individual cycles, especially the implementation, are checked, their effectiveness is measured, and appropriate corrective measures are taken by restarting the cycle. The cyclicality of public administration is described in the literature with the following formula:

POSDCoRB (Planning, Organizing, Staffing, Directing, Co-ordinating, Reporting, Budgeting)

The cyclic management of quality management systems also records these basic elements. ISO quality management systems are based on the quality management cycle, which is classically described by the standard with the formula PDCA (Plan, Do, Check, Act).

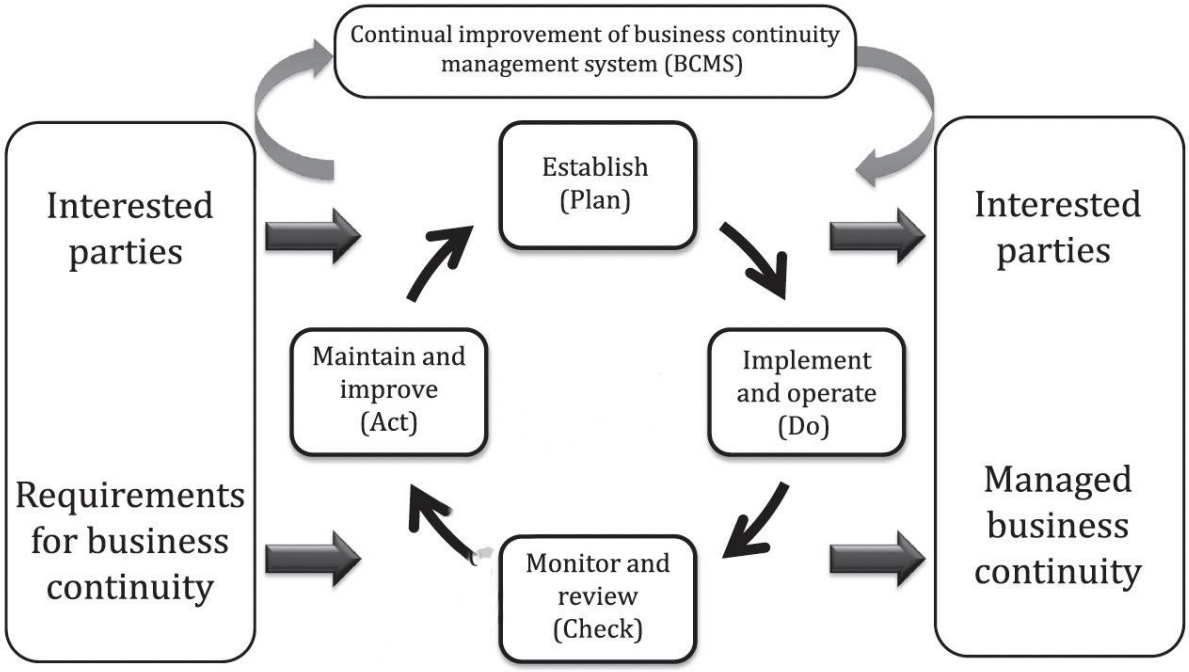

Figure 1. PDCA cycle applied to BCMS processes [1]

3. PRE-PLANNING STEPS

Prior to planning, as determined by the administrative cycles discussed above, objectives and information acquisition, as well as observation and analysis of the examined/planned system/process, are necessary. The standard achieves this through business impact analysis and risk assessments.

However, before carrying out the two processes, especially in a public administration system, in in-patient care, it is essential to set goals and identify business processes, which significantly determines all elements of the entire system cycle.

3.1. Objective: What am I planning?

To understand the relationship between the operator security planning tasks and the hospital disaster planning tasks with each other and with the emergency itself, we can get there by reviewing and interpreting the so-called critical infrastructure protection event cycle. [2]

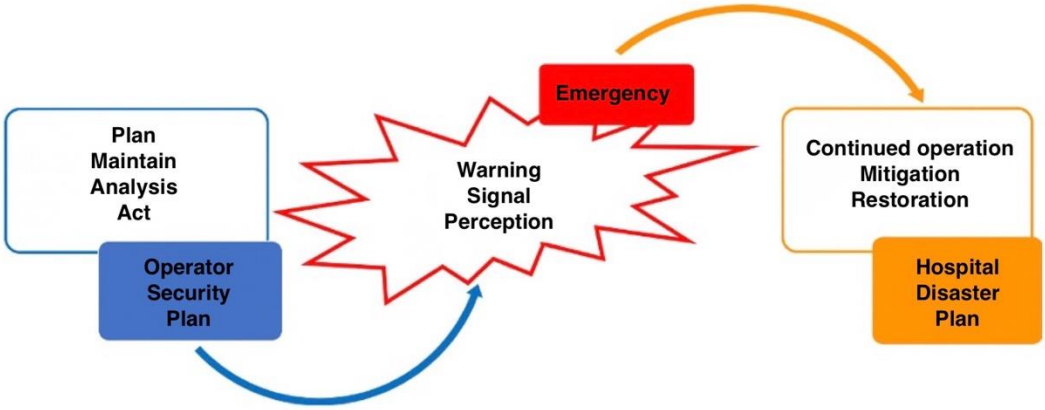

Figure 2. CIP event cycle[1]

The extraordinary event around which the cycle is built according to the law:

- a utility outage of more than 2 hours,
- all events affecting the infrastructure, defined in separate legislation, which lead to the cessation of the conditions necessary for operation or the transformation of the core activity,
- when the competent authority orders a health shutdown at the critical infrastructure element,
- the critical lack of human resources to such an extent that it can lead to the cessation or suspension of the activity. [3]

The planning tasks of the period before the extraordinary event, through operator security planning, cover the operator behavior and organizational tasks to be followed to prevent the extraordinary event, as well as the continuous measurement and evaluation of the risks of these processes and the appropriate interventions. During this period, it is necessary for us to create

[1] Mészáros, István, 2019.

plans and procedures regarding the behaviors and organizational tasks necessary for the management of an external or internal emergency event, the prevention, mitigation and restoration of the crisis, as well as for continuing operations. [4]

Security planning is therefore ideally done preventively before an extraordinary event occurs and is aimed at reducing the possible effects of the extraordinary event on human life and the basic processes of operation.

3.2. Objective: What I plan to protect?

It is characteristic of critical infrastructures that these facilities and the processes taking place here must function in all circumstances, the operation of these processes is essential from the point of view of the country's economy and society, based on the conditions of identification and designation. The focal point of planning and protection must therefore be the basic processes – the „business processes", how the standard call these – of the system element.

When introducing any new administrative system, it is primary to involve and convince management who have decision-making and action competence.

In order to support business continuity planning, it is necessary for management to be aware of the benefits of implementing the system:

- Mission Accomplishment: Organizations are created for a variety of purposes, from production to service. In all cases, the basis is the production of profit.
- The financial result: Perhaps the most important advantage of BCP systems, which is influenced by how long it takes and at what cost to restore the basic processes after an extraordinary event, and what loss of profit results from the stoppage of production.
- Loss Mitigation: The BCP process requires a thorough examination of potential losses against environmental hazards and threats.
- Customer-based approach: Authorities, businesses, organizations rely on customers, it is necessary that customers: patients, students survive the disaster and return.
- Human resources: Every business primarily relies on the people who work there. Since businesses invest in their human resources, businesses have a very high ethical

responsibility to protect not only people, but also the time and costs invested to them. [5]

The above principles of business continuity planning can already bring a new approach to the planning practice of in-patient care critical infrastructures, however, in my opinion, this approach needs to be further shaped, refined, and expanded. First of all, it is necessary to identify what I am investigating, what I am planning to protect, so what is my basic process. Of course, the financial loss can also be measured, however, in the case of a critical infrastructure element in the health sector, it is not possible to measure in terms of business balance sheet results the basic processes' the impact of a disturbing effects. Of course, these aspects should also be examined during the administrative cycle from the point of view of the planning and provision of resources. However, it must be stated that in the case of an in-patient care facility, the only profit for which I can create a security plan is the benefit of the patient. In my study, relying on this basic process, I would like to present the possibilities of introducing process-oriented BCP systems.

3.3. Obtaining information: Who am I planning with?

In order to be involved, it is primarily necessary to identify the value managers, i.e. the Stakeholders, as we will later carry out the planning and the analysis of the basic processes and their sub-processes with them.

Based 92nt he following methodology, a general Stakeholder-analysis of an in-patient care facility can be performed, in which the most important external and internal actors are listed, identified and analyzed one by one.

An example of evaluating the attributes of a Stakeholder::

	Personal involvement	*Level of support*	*Influence change*	*It can be influenced by us*
Director	Great – dedicated to its clinic/hospital	Supporting – within its enviroment, it does everything for operation	Medium – within budgetary frameworks along the principles of central management	Barely – it is responsible for the management of its organizational unit, as a leader it feels it can manage in all situations

Table 1. Stakeholder-analysis

During the visual presentation of the above analysis, the stakeholders can be placed in a coordinate system that can be made quasi-four-dimensional with the markings.

In this coordinate system, the participants can be placed based on their personal involvement and the degree of their support, and it can be clearly identified from these two values that they must be involved in a strategic or operational way during the planning, or that our task is only to give instructions or demand their contractual obligations.

The color and shape determine to what extent we can rely on their ideas, habits, and reflex-like reactions, as well as how and to what extent it is necessary for them to teach the plan and adjust their reactions after the planning.

Below is an example of a visual representation of a Stakeholder Analysis for a typical in-patient care facility.

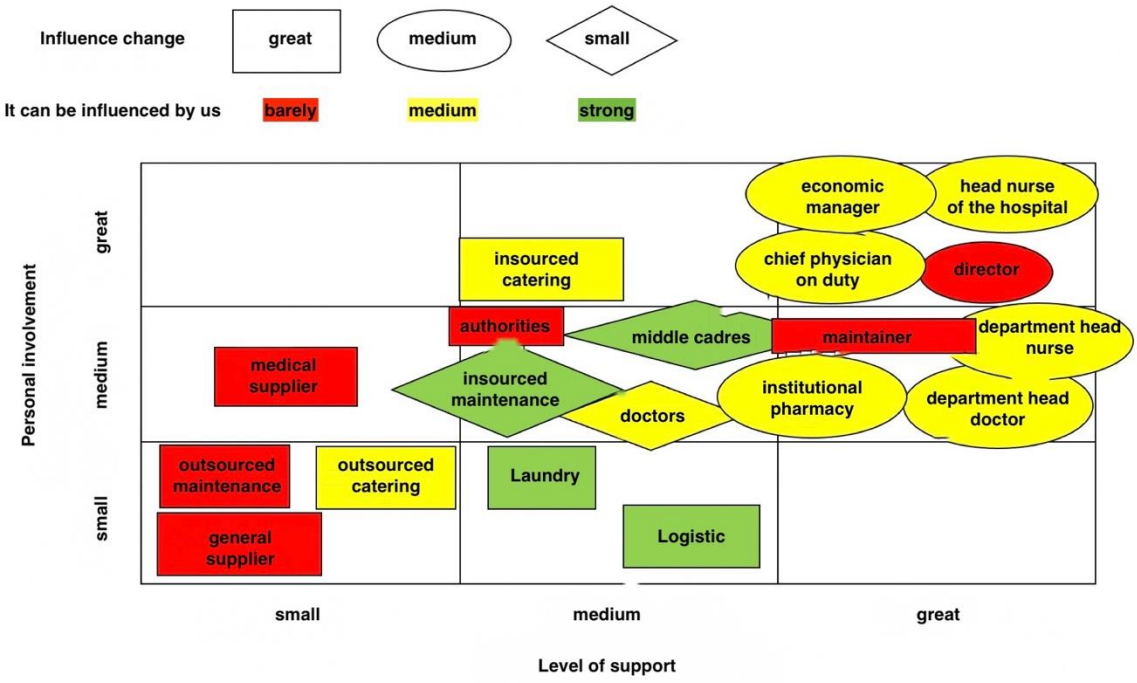

Figure 3. Visualisation of Stakeholder-analysis

The analysis also sheds light on the dependencies of the system and identifies key and critical stakeholders in the supply chain. After the analysis, it is necessary to conduct interviews with the stakeholders, the recommended methodology of which is to conduct the interviews starting from the upper right corner downwards and to the left, since these stakeholders have the greatest personal involvement, their attitude is the most supportive and they know the processes of the system element best.

3.4. Obtaining information: Business Impact Analysis (BIA)

Business impact analysis enables the organization to set priorities for resuming disrupted activities. Its main purpose is to enable the organization to identify and prioritize all activities that may require urgent intervention, if interrupted or disrupted, because failure to quickly resume or restore the given activity may result in unacceptable levels of adverse effects. [6]

The five steps of the BIA:

- Obtaining management support;
- Understanding the organization;

- Application of BIA tools;
- BIA process;
- BIA results.

The main purposes of the BIA:

- BIA is necessary for the development of the business continuity management system;
- It is key to understanding the context of the organization;
- BIA identifies the financial and operational loss of the organization's business functions;
- Provides data to establish Maximum Tolerable Downtime (MTD), Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO).
- BIA provides a basis for management to select the most cost-effective continuity strategies;
- Identifies gaps in prevention, preparedness, response, mitigation and recovery. [7]

This can be achieved primarily through interviews with stakeholders. The purpose of the interviews, as defined above, is to explore daily operations, resource requirements, responsibilities, and the potential impact of a disruptive event.

In addition to interviews, other applicable methods are::

- Review of documentation;
- Making a survey and questionnaire;
- Holding a workshop discussion;
- Holding and evaluating a scenario-based exercise. [8]

3.4.1. Flowcharts

On the basis of the information obtained during the information gathering, in order to continue the business impact analysis and to illustrate the revealed processes, it is advisable to create flowcharts, on which we mark the identified base and sub-processes, the impact analysis of which is carried out.

Tasks:

- Identification of the basic process:
    - patient care

- Identification sub-processes:
  - diagnostic
  - in-patient care
  - out-patient care
  - surgeries
- Identification of the supplier processes:
  - maintaining of facility
  - patient catering
  - maintaining of medical devices
  - healthcare textile supply
  - dangerous waste management stb.

Planning must be done for all sub-processes, even if most of the sub-processes appear in more than one basic process. Because the disruption of the same partial process can have different effects on the given basic process, and the determination of the recovery values can also differ, which in the case of the given sub-processes must be planned in accordance with the given basic process.

3.4.2. Criticality ranking

Prioritizing criticality means providing processes with metrics, which requires the establishment of a system of criteria. The ranking of criticality can be done primarily on the basis of the impact on our basic process, which of course requires that we interpret it for the given process. However, the legal environment also provides a basis for defining the criteria system, which determines both the horizontal and sector-specific criteria for designation as critical infrastructure.

During the identification procedure, the authorities involved in the decision decide on the designation as critical infrastructure based on this set of criteria.

Based on the legislation, the horizontal criteria:

- criteria for losses,
- criteria for economical effect,
- criteria for social effect,
- criteria for political effect,
- criteria for enviromental effect,
- criteria for protection.

It is essential that the management is able to apply this complex system of criteria to the identified processes in a hospital environment. Thus, the focus remains on patient care. In this case, it is difficult to measure the effect of disturbances, since if we take the care and recovery of patients as a basis, then it is obviously neither measurable nor acceptable to measure how many patients do not recover in the case of a disturbing effect, perhaps as a result of insufficient treatment what negative personal consequences are there. On the other hand, during the examination of the processes and sub-processes at the level of the national supply, or the territorial supply obligation of a hospital, it is possible to examine, in which case, which process and to what extent has effect.

A good example of this is the current pandemic caused by the coronavirus, for which, although there were no plans, the processes of business impact analysis can still be identified in the decisions of professional management. In order to ensure the care of patients suffering from the coronavirus disease (human resources and bed capacity insurance), screening tests were first suspended, and later forms of inpatient care requiring non-acute care and surgical activities were suspended. Appropriate planning is essential, however, because although the process criticality can be prioritized by the supervisor in an ad hoc manner, it is necessary to plan with the long-term effects of the stopped processes in mind, including establishing the maximum tolerable value of the stoppage based on the above set of criteria.

3.4.3. Tolerable downtime and recovery time objectives

Based on the above, the maximum tolerable downtime, the recovery point, where the recovery can still begin, and the required recovery time must be determined and assigned a value for each process and sub-process.

After identifying the processes, it is necessary to determine the following values for each process with the most involved strategic stakeholders:

- MAO (Maximum Tolerable Outage)/MTD (Maximum Tolreable Downtime)
- RTO (Recovery Time Objective)
- RPO (Recovey Point Objective): where the recovery of the process can be done within the MTD taking into account the RTO

The risk assessment can only begin after these values have been defined and prioritized.

4. OBTAINING INFORMATION: RISK ANALYSIS

The purpose of the risk assessment is to determine whether we plan to reduce or eliminate the risk during the planning process, or whether we live with it, so it does not require any action other than continuous monitoring.

The risks of the basic processes can also be approached from the professional minimum conditions required for the provision of health services and from the operational side of the facility. During the preparation of the OSP, it is necessary to use both approaches in order to assess the real capabilities, especially considering that some elements of the two approaches are closely related to each other.

Thus, it is definitely necessary to assess from the side of minimum conditions and analyze from the side of risk:

- The number and availability of medical personnel;
- The number of necessary medical devices, their maintenance, suitability for use;
- The local characteristics of the provision of medicine, sanitary textiles, laundry, and food.

From the facility operation side:

- Water, electrical energy, gas, medical gas, steam and sewer service methods and possible redundancies;
- The maintenance of the facility and the devices included in its operation, as well as the conditions for planned preventive maintenance and troubleshooting;
- Elevators and other personal and material handling devices;
- Plans for failure of the above;
- The method of waste management with particular attention to chemical and infectious hazardous waste;
- How to handle hazardous materials;
- The availability, familiarity and applicability of the protection type regulations of the organization (labor, fire, property, environmental and civil protection, IT security), as well as the documents of the quality management system.

- IT and other communication devices and networks, and their security.

When assessing external risk factors, it is especially necessary to assess the following.

- Presentation of the operating environment of the designated critical infrastructure;
  - Geographical enviroment;
  - The population of the district, offices, public institutions, services;
- The natural vulnerability of the operating environment of the designated critical infrastructure;
  - Hazards related to water circulation (groundwater, inland water, flood);
  - Risk of geological origin;
  - Risk of meteorological origin (including typical wind directions);
- Civilizational, industrial and communal endangerment of the operational environment of the designated critical infrastructure;
  - Danger from traffic and transportation;
  - Presentation and vulnerability of services and infrastructures that ensure the basic supply of the population and the operation of critical infrastructure;
  - The situation of the district's utilities and energy supply;
  - Infocommunication services, network supply;
- Dangers of other origin;
  - Hazardous plants, factories, and power plants that have an influence on the operation of the designated system element are located in the vicinity;
  - Classification of the district into a disaster management class. [9]

The general form document sent by the National Directorate General for Disaster Management (NDGDM) in 2020 to the operators of critical infrastructures breaks down the risks to be assessed into the following main groups:

- meteorological risks,
- geological risks,
- human risks,
- technical risks,
- communication risks,
- case of fire,

- IT risks,
- risks of dangerous materials origin,
- other risks specific to the given sector.

Given that this is a general form, as mentioned in the last line, it is also necessary to assess and evaluate sector-specific risks on the part of the given operator. Here, it is possible to examine the risk from the side of the minimum conditions and the processes that serve them, so in the case of a vital system element for inpatient care, these could be the following:

- error in medical devices
- safety of elevators and other patient handling devices
    - elevators (especially considering their number and the number of safety elevators)
    - manual patient handling devices (with particular regard to their availability and usability)
- patient catering
    - according to normal operation
    - according to Hospital Disaster Plan
- sanitary textile and laundry
- medical gas
    - oxygen
    - vacuum
    - compressed air
- ventilation systems (especially with regard to the replacement of air filters, the required number of air changes, germ-free operation and their measurement)
- drug supply
- blood, blood product, laboratory sample supply, delivery
- Other medical material supply (personal protective equipment, test tubes, diapers, formulas, dressings, etc.)
- cleaning

- healthcare (infectious), chemically hazardous and municipal waste (with particular regard to their internal management, occupational accidents resulting from them, risk factors)

The form document issued by NDGDM uses the following formula to evaluate risks:

The value of the risk (RV) = risk probability (RP) (1-5) * (risk impact (RI) (1-5) + exposure (EX) (0-2))

RV = RP * (RI+EX)

Based on the risk value obtained on the basis of the formula, the operator can decide whether to live with the given risk without taking measures or to take measures with the necessary urgency:

- 20-25: take measures with the necessary urgency
- 15-19: take preventive protectional measures
- 10-14: requires action
- 5-9: planned, subsequent action
- 1-4: negligible risk

If, in the case of the given risk, the operator of the critical infrastructure is apparently unable to reduce it to an acceptable level within its competence, the situation assessment and action by the specialist authority and the sectoral arbitration committee are essential.

„The services used by the critical infrastructure from third parties may influence the service provided by the operator, or may have an impact on the continuous operation of the system element. These are taken into account by the formula in a weighted manner (in general, it can be said that according to the above methodology, the resulting value increases by at least one risk category as a result of the weighting). The exposure can be reduced, for example, by concluding partner agreements (SLAs) providing adequate guarantees, which can reduce the residual risk value to an appropriate level as a risk-reducing measure.” [10] However, exposure can arise not only towards contracted partners (although this is also the case with the dependent critical infrastructure that appears as a utility provider), but also internally, from the interdependence of our own processes. That is why it is advisable to replace the exposure value with a dependency value during the process-based approach.

During the business impact analysis, we established the basic process and main processes of critical in-patient care infrastructure. All this in order to establish the maximum tolerable value of their outage, as well as the last recoverable state and the recovery time for these main processes. The risks for these processes must be evaluated individually and the interdependencies of the processes must also be taken into account. Based on these, the risk of the individual sub-processes can also be determined in relation to each other. The interdependent nature of the main processes within the healthcare and inpatient care infrastructure is shown in the figure below:

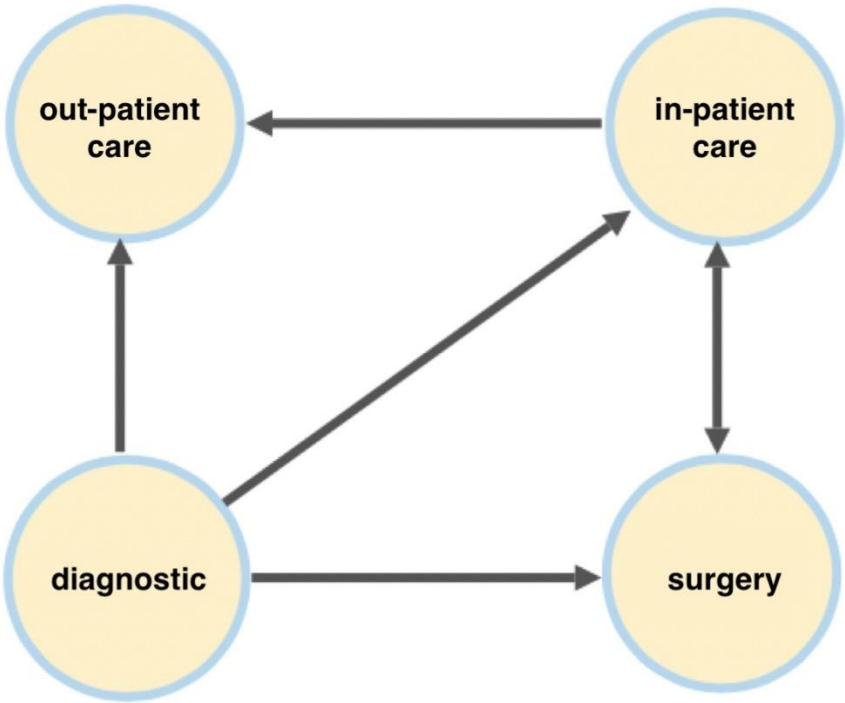

Figure 4. Interdependencies of a hospital's processes[2]

A specific examination of interdependencies based on risk assessments is also necessary across sectors. The interdependency is „a bidirectional relationship between two infrastructures through which the state of each infrastructure influences or is correlated to the state of the other. More generally, two infrastructures are interdependent when each is dependent on the other. ... This definition suggests that the operability of one infrastructure can be contingent on the operability of another. It has also been suggested that infrastructure interdependencies increase

[2] Mészáros, István, 2021.

the overall structure, contribute to system complexity and could be a basis for systems of systems, whose functionalities depend on the performance of the constituent interdependent systems. This notion supports the proposition that the goal of maintaining and sustaining public wellbeing, including health, economy and security, depends on the inputs and outputs of multiple highly-interconnected systems.The relationships among such infrastructures are not one-to-one, but multidirectional. Therefore, risk formulation in such infrastructures should consider the bidirectional nature of relationships among critical infrastructures." [11]

5. PLANNING

The planning consists of several parts, which result in the creation of the complex Business Continuity Plan.

The identification of business continuity foundations and the selection of business continuity solutions must be done through a business impact analysis and a risk assessment that takes into account the related costs, so through the concepts learned in the information gathering phase, the plan consists of the following parts:

- risk assessment action plan intended to reduce risks
- emergency management plan
- plan of operation under disaster conditions – Hospital Disaster Plan
- de-escalation planning, during which the system element is restored to "peacetime" operation

The purpose of the planning is therefore to reduce risks, to enable the organization to ensure that the individual sub-processes can only be stopped for the maximum tolerable time specified in the business impact analysis for the duration of an extraordinary event and can be restored at the specified point. The basic process within the framework of crisis healthcare can be operable.

At the level of the central health administration, the purpose of collecting and analyzing the plans is to increase the maximum tolerable shutdown values at the national level, to group the necessary forces and tools in the direction of critical infrastructures through relocation, and to plan all of this.

„Each business continuity plan should identify its purpose, scope and objectives in a form that is clear to the teams that use it. Links to other rquired or relevant documented procedures or documents should be clearly stated and the method of obtaining and accessing them described. The business continuity plan should also include:

- activation criteria and procedures;
- implementation procedures;
- communication requirements and procedures;
- internal and external interdependecies and interactions;
- resource requirements;
- reporting requirements;
- information flow and documentation processes.” [12]

6. DECISION

In order to reduce certain risks and to implement the crisis health activity, several alternative options can be considered, the priority order of which needs to be determined, and it is necessary to decide which one will be implemented first. This decision depends on the budget resources and the support of the sectorial manager (material, asset, force allocation).

We found that the general business process-based approach, which focuses on the maximization of financial profit, cannot be applied in healthcare, since the profit of the basic processes of healthcare institutions is the patient's health and life, which cannot be measured in money. During the decision, the only financial consideration is the budget framework of the inpatient care institution which - seeing the hospital debt that accumulates again and again every year - is otherwise insufficient for operation.

This decision is actually the issuing of the above in the form of a planning system by the operator, i.e. the manager of the critical infrastructure.

With the issuing, and thus with the decision, the persons responsible for the risk reduction measures, their deadline, and the budgetary resources necessary for the implementation are

assigned. The leaders and task forces responsible for the implementation of extraordinary events and crisis health activities will be determined.

7. IMPLEMENTATION

The implementation of the planning system is generally the assignment, acquisition and securing of the executive staff as force and tools for the given task.

Based on the planning system of the health institutions, the implementation can be divided into two parts:

- "Peace time" implementation: This is mainly the implementation of business continuity, i.e. risk reduction measures, the provision of personnel and equipment, the provision of budgetary resources assigned during the decision, the execution of purchases, public procurement.
- „Health care crisis time” implementation: This is the application of the Hospital Disaster Plan and its sub-plans that fit the extraordinary event, in accordance with the plans and in an internal and external cooperation order.

8. COORDINATION

Coordination means the coordination of plans and implementation. According to the implementation, it can also be divided into two parts.

- "Peace time" implementation: It refers to the coordination of various sectoral development programs, institutional development plans and risk management measures, as well as institutional and central public procurement activities.
- „Health care crisis time” implementation: In this case, on the one hand, stronger central coordination will appear, as the operation and management and cooperation systems of the entire health administration will change, and on the other hand, the management of the institutional hospital disaster activity will also be transferred to the senior

management system designated in the plans, which will also change the usual task assignment and reporting routes.

9. CONTROL

It is essential during the control:

- Review the business impact analysis at regular intervals;
- Review the risk analysis at regular intervals;
- Checking the knowledge of employees;
- One of the most effective and practical ways of control - primarily in the case of extraordinary event management, recovery and hospital disaster planning - is the exercising.

In general, questions to be asked during the inspection:

- Do the risk values, the overall potential losses, decrease?
    - Probability of occurrence.
    - Value of the potential damage.
    - The exposures.
- Have we increased the maximum tolerable shutdown value?
- Have we postponed the last possible start date of the reset?
- Have we reduced the time required to restore?
- So overall, is the entire system safer?

With the help of the Key Performance Indicators (KPI) used during the audit, we can measure the effectiveness of our business continuity systems.

Such a main performance indicator can be developed for all the questions to be asked during the inspection defined above. According to some, the requirement for effective measurement is based on a wider range of measured data, i.e. collecting as many metrics and additional information as possible, from as many places as possible, while other experts believe that the quality of the data is more important than the quantity. According to the latter point of view, the measurement objectives must be SMART and DUMB at the same time, i.e. the requirements

for the measurement objectives are Specificity, Measurability, Availability, Relevancy and Time-basing, as well as Doability, Understandability, Manageability and Beneficiality. [13]

10. SUMMARY

A change of approach can be achieved in the operator security planning of the critical infrastructures of the healthcare sector, which is required by law, and the efficiency of planning and operation can be increased by using quality management systems, including business continuity management systems.

In my study, I pointed out that the first milestone in the operation of business continuity systems is planning, which, however, must be preceded by the designation of the objective and the acquisition of information. For this, it is of primary importance to convince the management, to identify the stakeholders who can provide the appropriate information and participate in the planning, then together with these stakeholders, the basic processes and the business impact analysis of their disruption, i.e. the exploration of the impact on the basic process, must be identified.

After that, I revealed that the risk assessment that begins after the business impact analysis must cover each and every process and in which the critical paths, the individual risks and threats can be prioritized based on the established maximum acceptable shutdown values. A complex action plan can then be prepared based on the identified risks, the prioritization of criticality, the consideration of interdependencies, and the tolerable shutdown and necessary recovery values.

After the planning phase, in the decision-making phase, we must return to our basic principle stated during the planning of the business continuity systems of healthcare critical infrastructures, during which we established that the benefit of the basic processes of healthcare institutions is the health and life of the patient, which cannot be measured in money, so risk management decisions are can not be applied on based of the cost-benefit principle.

In order for the complex business continuity system, i.e. the Operator Security Plan and Hospital Disaster Plan required by law, to be practical and applicable in practice, it is essential

to check the plan system and measure its effectiveness. The most appropriate tool for this is the implementation of complex practices prescribed by law, but not used in the case of health critical infrastructures in operator and official practice.

REFERENCES

[1] ISO 22313:2020, ix. p.

[2] Dr. Major László: A katasztrófa-készenlét, a reagálás és a beavatkozásbiztonság egészségügyi alapjai. Budapest, Semmelweis Kiadó, 2019. 66. p.

[3] Decree 246/2015. (IX. 8.) of Government on the identification, designation and protection of essential healthcare systems and facilities

[4] Dr. Major László: A katasztrófa-készenlét, a reagálás és a beavatkozásbiztonság egészségügyi alapjai. Budapest, Semmelweis Kiadó, 2019. 66. p.

[5] Brenda D. Phillips, Mark Landahl: Business Continuity Planning: Increasing Workplace Resilience to Disasters. Oxford, Elsevier, 2021.

[6] ISO 22301:2020, 20 p.

[7] Eugen Tucker: Business Continuity from Preparedness to Recovery. Oxford, Elsevier, 2021. 70.

[8] ISO/TS 22317:2015 Annex C 20 p.

[9] Dr. Kátai-Urbán, Lajos, Mészáros, István, Dr. Vass, Gyula: Iparbiztonság, válsághelyzeti tervezés in: Dr. Major László: A katasztrófa-készenlét, a reagálás és a beavatkozásbiztonság egészségügyi alapjai. Budapest, Semmelweis Kiadó, 2019. 68-69. p.

[10] Instructions for completing the risk analysis, Ministry of Interior NDGDM, 2021.

[11] Katina, Polinpapilinho & Pinto, C Ariel & Bradley, Joseph & Hester, Patrick: Interdependency-Induced Risk with Applications to Healthcare. International Journal of Critical Infrastructure Protection. 2014. 7. 10.1016/j.ijcip.2014.01.005.

[12] ISO 22313:2020 40 p.

[13] BSI UK: Measurement matters - The role of metrics in ISO 22301 - A BSI whitepaper for business. 2015. 4.

Mészáros István

PhD hallgató – Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola,

műszaki főigazgató - Semmelweis Egyetem,

meszaros.istvan.mail@gmail.com, ORCID: 0000-0002-1555-0705

István Mészáros

PhD student – Ludovika University of Public Service Doctoral School of Military Sciences and Military Engineering,

General Director of Technical Affairs – Semmelweis University,
meszaros.istvan.mail@gmail.com, ORCID: 0000-0002-1555-0705