GIS Odyssey Journal

2022 • Volume 2 • Number 1

https://doi.org/10.57599/gisoj.2022.2.1.39

Jerzy Stanik[1], Maciej Kiedrowicz[2]

RISK IN GIS SYSTEMS

Abstract: The development of information technologies, widespread access to the Internet, globalisation and the development of measurement technologies in geodesy, on the one hand, result in wide access to geographical, cartographic or geodetic data, and on the other hand, increase the level of risk of losing basic security attributes of these data. Risk management in GIS should be implemented at every stage of the GIS life cycle, which starts with the organising phase of a GIS and is expected to continue until the end of its life – decommissioning. It is important to remember that it is not enough to have a good analysis and assessment of adverse events and their consequences without precise, pre-developed methods of measuring and responding to risks in the form of various response plans. This article is an attempt to answer the questions: what should be understood by risk in GIS systems, how to measure it and how to proceed to manage it effectively and efficiently. The models and instruments presented, which have been developed on the basis of available literature and own research, point the way to effective risk management in GIS class systems.

Keywords: spatial information system, risk, information security, risk management system, security configuration, Statement of Applicability (SoA)

Received: 13 June 2022; accepted: 30 June 2022

[1] Military University of Technology, Faculty of Cybernetics, Institute of Computer and Information Systems, Warsaw, Poland, ORCI ID: 0000-0002-0162-2579, email: jerzy.stanik@wat.edu.pl
[2] Military University of Technology, Faculty of Cybernetics, Institute of Computer and Information Systems, Warsaw, Poland, ORCI ID: 0000-0002-4389-0774, email: maciej.kiedrowicz@wat.edu.pl

Introduction

Modern geographic information systems (GIS) have, on the one hand, become very powerful technologies because they allow geographers to integrate their data and methods in ways that support traditional forms of geographic analysis as well as new types of analysis and modelling that go beyond the capabilities of manual methods, while on the other hand they have become more vulnerable to various cyber attacks. The consequences of cyber attacks most often manifest themselves in the leakage of sensitive data. The actions of criminals can also affect the stability of GIS systems and even cause them to lose business continuity or suffer long-term damage. This negatively affects all procedures, regardless of GIS class.

The effective operation of cyber security in a GIS environment involves implementing and coordinating appropriate solutions across the information system. Cyber security activities include providing security in areas such as networks and applications, endpoint protection, geodata, identity management, databases and infrastructure, cloud data, disaster recovery, technical security of the company network, system and server architecture, remote connection to the company server.

The ever-changing nature of threats is recognised as one of the more difficult challenges in GIS cyber security. Traditionally, actors focus most of their cyber security resources on protecting only their most important system components, in order to defend against known threats (Wróblewski, 2015). Today, this approach is insufficient as GIS threats are advancing and changing faster than organisations can keep up. As a result of the above, more proactive and adaptive approaches to cyber security and risk management in GIS cyber security should be promoted. Most people involved in cyber security recommend a move towards continuous monitoring and real-time threat assessments, to an approach based on elements of good practice and a data-driven approach to cyber security, as opposed to the traditional model.

Cyber security today requires a new approach to risk management, based on understanding the strengths and weaknesses of an entity of operation, e.g.: a GIS system, and based on this, developing effective cyber defence methods. Conscious management of the security area, bearing in mind limited and hard-to-reach resources, requires risk analysis and prioritisation of threats.

Risk management in GIS is a complex, interdisciplinary field (related to computer science, mathematics, statistics, finance and management). In general, risk management in GIS class systems increases the value of the GIS, and by increasing the value of the many components of the GIS system, there is ultimately an increase in value – added value – for the entire entity of operation that operates the system. The current trend is to manage both GIS information systems risk and GIS itself simultaneously, as one integrated GIS management process. There are many levels of integration, but this integrated measurement is the key point of this article. This is a difficult problem due to the variety of types and measures of risk of the underlying GIS components.

The multifaceted nature of the issue of GIS cyber security means that the issue is increasingly being considered not only in the area of protecting key information systems

and elements of the GIS technical architecture, but also from the perspective of the impact of the adopted GIS security model and risk management system lifecycle model on the choice of risk management strategy.

The aim of this paper is to present two models: a GIS security model and a risk management system lifecycle model for GIS. In the opinion of the authors, these models can help in a good effective method of risk estimation and handling strategy. The results obtained from the implementation of the risk estimation and handling strategy process provide a strong basis for the development of the Statement of Applicability document and then how to map the service strategies provided in ISO 27001 to the controls of ISO 27001 – Annex A. The Statement of Applicability is a basic requirement for ISO 27001 certification. This is a statement explaining which security controls in Annex A do or do not apply to the information security management system in GIS class systems.

GIS security system

GIS is one of the many information technologies that have changed the way geographers conduct research and contribute to the information society. GIS is (Aranoff, 1989 and Peggion et al., 2008) "an organized set of computer hardware, software, geographic data and personnel designed to efficiently capture, store, update, manipulate, analyze and display all forms of geographically referenced information".

System security management is an integral part of system management and is related to rationalisation of the selection of measures (methods, technologies) to ensure safe (as intended) operation of the system in a hazardous environment (environment). If there are no external threats, then system security management can be reduced to the problem of managing the reliability of the system: the choice should be made of such a reliability strategy for which the value of the reliability assessment criterion (system reliability function) assumes a maximum value under the condition that the costs of increasing reliability (or maintaining reliability at the desired level) do not exceed the limit (acceptable) – Figure 1. However, if there is a threat to the security of the system, then the problem of safety management can be reduced to the selection of such a safety strategy (measures to protect the system against threats) from a set of acceptable strategies, for which, for example, the expected value of the effects (losses) of threats assumes the minimum value under the condition that the costs of the strategy (implementation of protective measures) do not exceed the limit (acceptable) value. It should be noted that both the problem of reliability management and the problem of system security management can be reduced to the problem of: (1) minimisation of the risk function provided that the value of the effects (utility) obtained thanks to the functioning of the system is not less than the limit (desired) value or (2) maximisation of the system efficiency function provided that the risk function does not exceed the permissible ("safe") value.

In the system security analysis it was assumed that the effectiveness of the GIS system is influenced by (Sienkiewicz, 2005 and 2013):

- System reliability, i.e. the ability to function efficiently (without damage, failure, errors, etc.) under specific conditions, e.g. time:
- Cyber security of the system, i.e. the ability to effectively protect against the effects of cyber threats;
- Business continuity, i.e. the ability to anticipate and respond to incidents and disruptions related to operations so that operations can continue at an acceptable level.

A diagram illustrating the relationship between risk management, security barriers, reliability, and business continuity of a GIS system, for a reasonable level of risk, is shown in Figure 1.

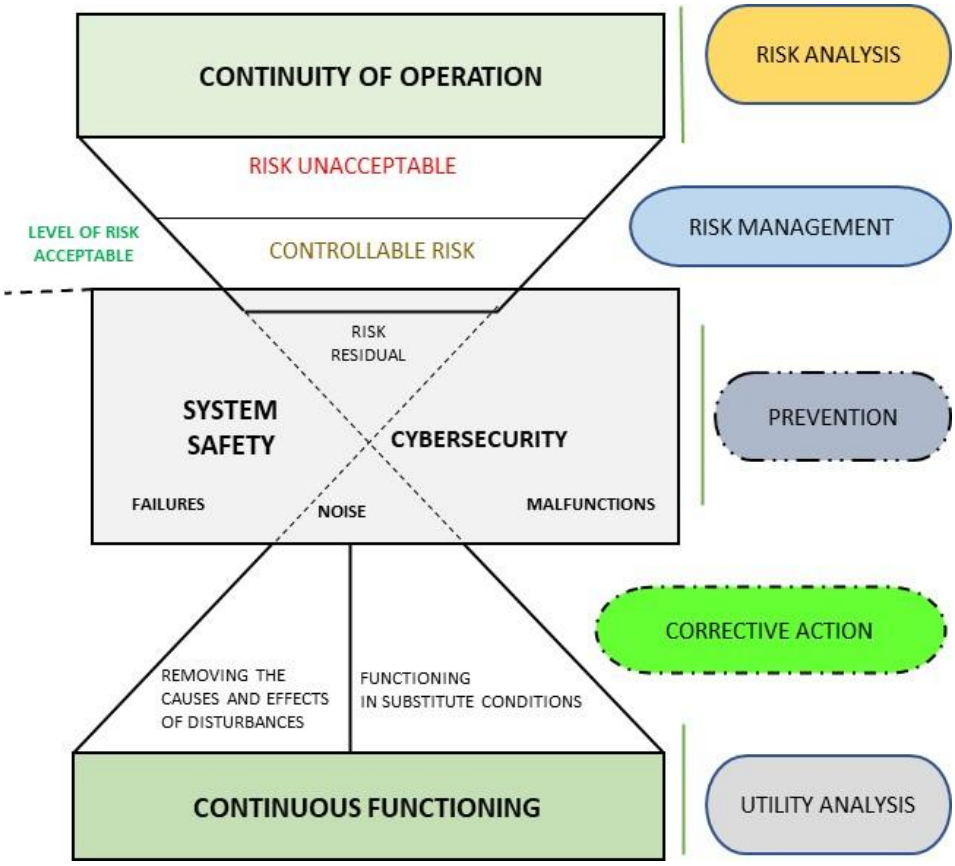

Fig. 1. Relationship between risk management, security barriers, reliability, and business continuity of the GIS for a reasonable level of risk
Source: The author's own elaboration

Keeping in mind the principles of good practice, we can assume that the best practice from the point of view of GIS information security is multiple layers of protection (Fig. 2). Caution: A high level of protection should not be expected from only one layer of defence.

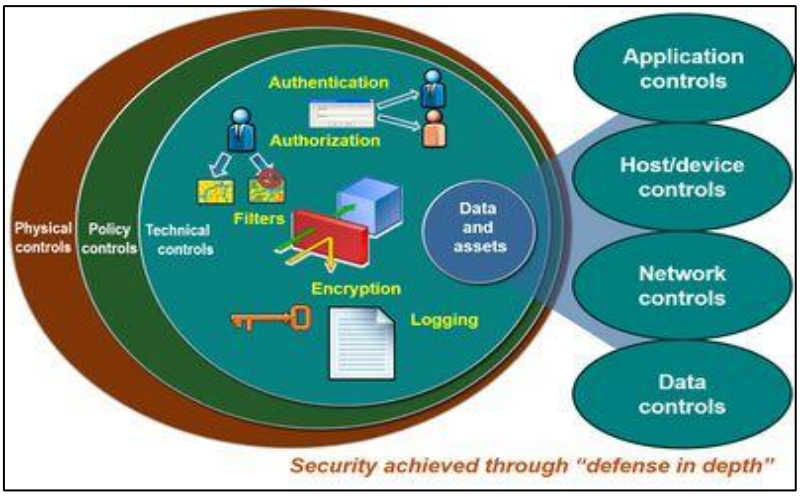

Fig. 2. Several security levels are required to ensure the protection of GIS business operations
Source: http://wiki.gis.com/wiki/index.php/Information_Security

The general security and risk management model of the GIS system is presented in Figure 3.

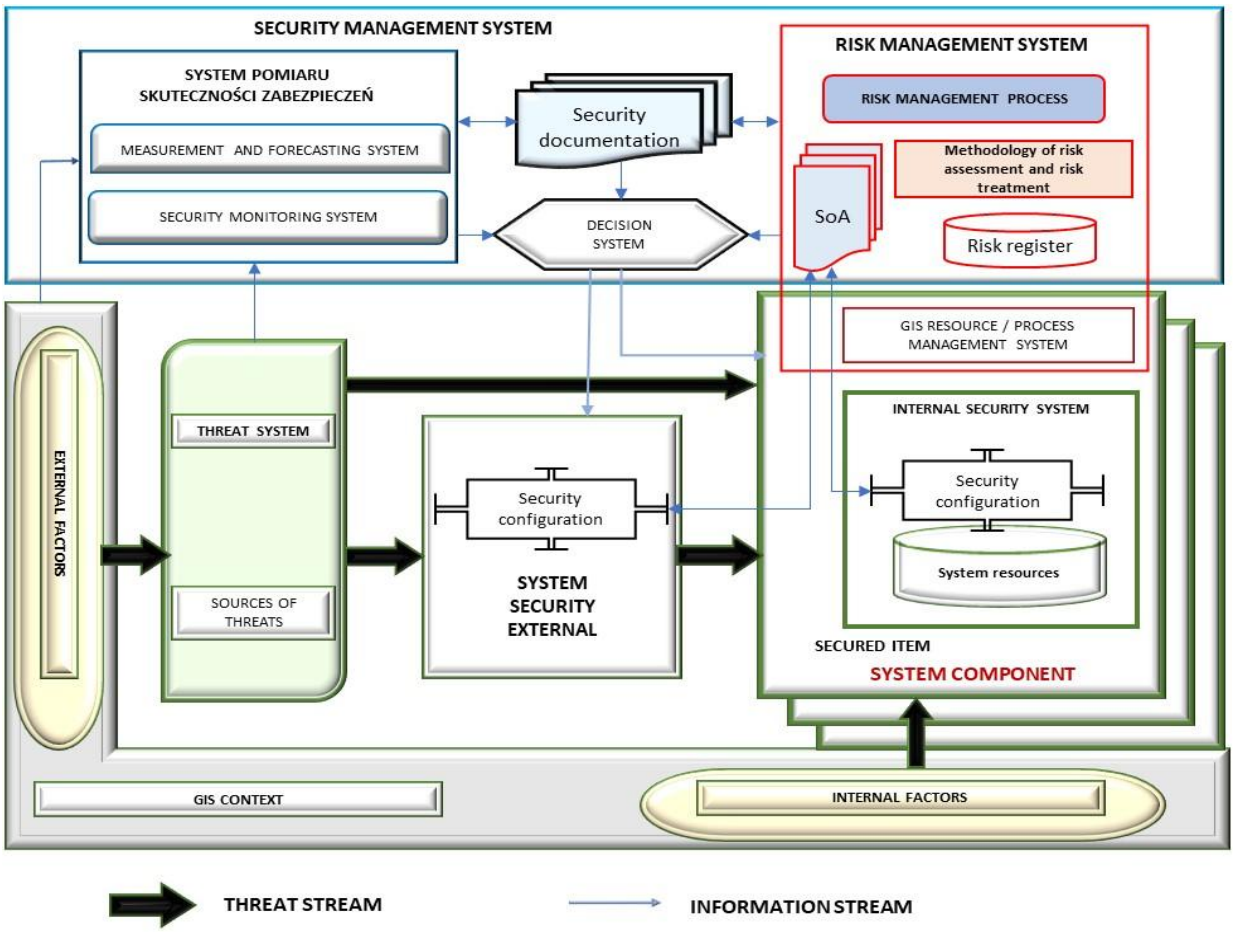

Fig. 3. General security and risk management model of the GIS system
Source: The author's own elaboration

GIS security is a property characterising the resistance to the emergence of hazardous situations, i.e. those in which the need arises to protect the internal values of the GIS system from external threats or threat factors. It was assumed that the general model of the GIS security system consists of components such as:

- The GIS context which is the set of all internal and external factors that affect the operation of the GIS and the effectiveness of achieving the objectives adopted by it. The external context includes the following factors: relations with external entities of GIS operation; external environment affecting GIS objectives: legal, financial, economic, technological. Internal context factors include: the configuration of the GIS, the resources at the disposal of the GIS (including information resources, financial resources, personnel resources, IT facilities and buildings), and the organisational chart with the division of responsibilities and roles in the GIS.
- The threat system (a set of threat sources and relationships between them) which is a specific threat generator.
- A system being secured (a threat object) having system resources of a certain value, protected by an internal protection system (a set of technical and organisational protections and relations between them).
- Security management system ensuring control of the external (superior) security system.
- Risk management system – GIS providing the GIS platform assets with an independent and cost-effective solution for all their information security and risk management requirements; the GIS risk management system can also be considered as a tool for addressing specific aspects of risk management.

A schematic illustration of the technical architecture of the GIS platform is shown in Figure 4.

There are currently several examples of integrated risk management applications, such as Risk-GIS. Developing a fusion between security, risk management philosophy and the power of GIS as a decision support tool has obvious practical applications and advantages. The purpose of Risk-GIS is to assist in decision making and problem solving in areas that affect the security and sustainability of communities. As such, it is an analytical 'engine' that drives the operational risk assessment process. It also provides a stronger form of risk communication through the ability to visually represent the risk situation.

There are many levels of integration of the Risk System with the GIS, but it is the comprehensive risk system model and integrated measurement that is the key point of this paper. This is a difficult problem due to the variety of types of risk system models and risk measures.

The security management process with the risk system can be considered as the relationship between the threat source, threats, security features, vulnerabilities and the threat objects of the technical architecture of the GIS platform with their vulnerabilities. Each local GIS subsystem informs the superordinate management system about the state of its security and forecasted threats.

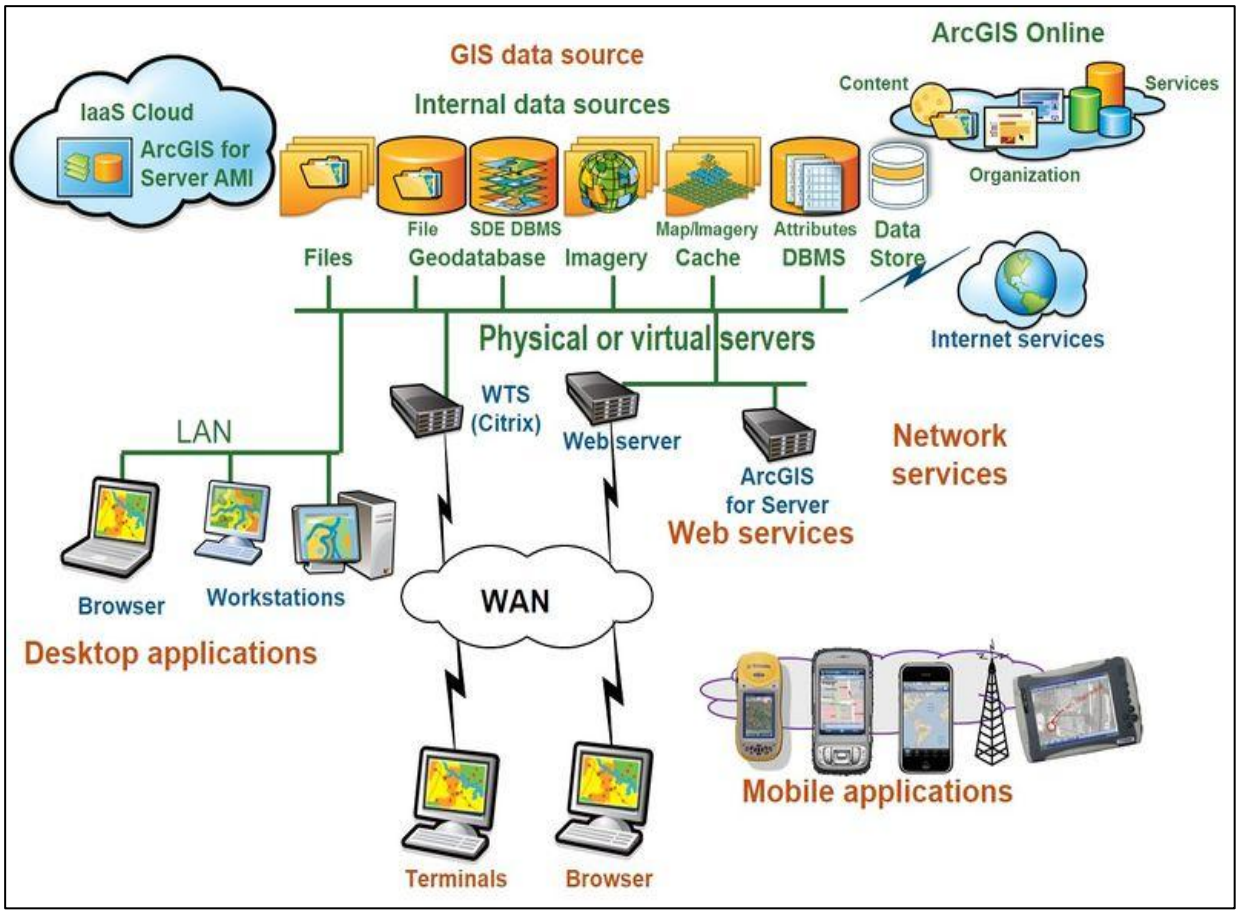

Fig. 4. Illustration of the technical architecture of the GIS platform.
Source: http://wiki.gis.com/wiki/index.php/Information_Security

The master system, on the basis of information about the state of the threat system and information about the local states of the GIS subsystems, plans a set of necessary security mechanisms of the external security system that can ensure effective protection of the resources of the GIS technical architecture.

In order to implement undertakings to ensure the required security level of GIS subsystems within the framework of an acceptable GIS security strategy, the master system should include the following subsystems:

- Decision-making system: allocates appropriate security configurations for the protection of local systems within an acceptable information security risk management strategy;
- Monitoring system: collects current information about the state of the GIS security system and identifies threat symptoms;
- Security level measurement and forecasting system: provides a basis for action planning;
- Risk management system: provides risk assessment and plans risk treatment and risk minimisation measures, which forms the basis for determining acceptable security strategies.

In the context of the above generalised model, the value of risk depends on threats, vulnerability (immunity) to threats, security gaps and the severity of the effects of threats. If threats have been identified, then a condition of system security is that the system is equipped with a certain defensive potential (resilience). In particular, it may be expressed by a specific, usually layered, system of protection against threats.

Standard approach to security risk management in GIS

Risk management as well as quality, resilience, business continuity and security management of GIS should be regular and continuous (Gregoriou et al., 2010), it should take place in a certain cycle consisting of phases, stages, processes and activities. Taking the number of distinguished stages in the life cycle of a risk management system as a criterion, we can distinguish many different models of risk management in GIS security, e.g. four-phase models, five-stage models, six-stage models, etc.

A common criterion for the subdivision/classification of security risk management models is the way in which security risk management is approached and/or the risk assessment methodology and strategy for dealing with risks. Standard approaches to security risk management are shown in Figure 5.

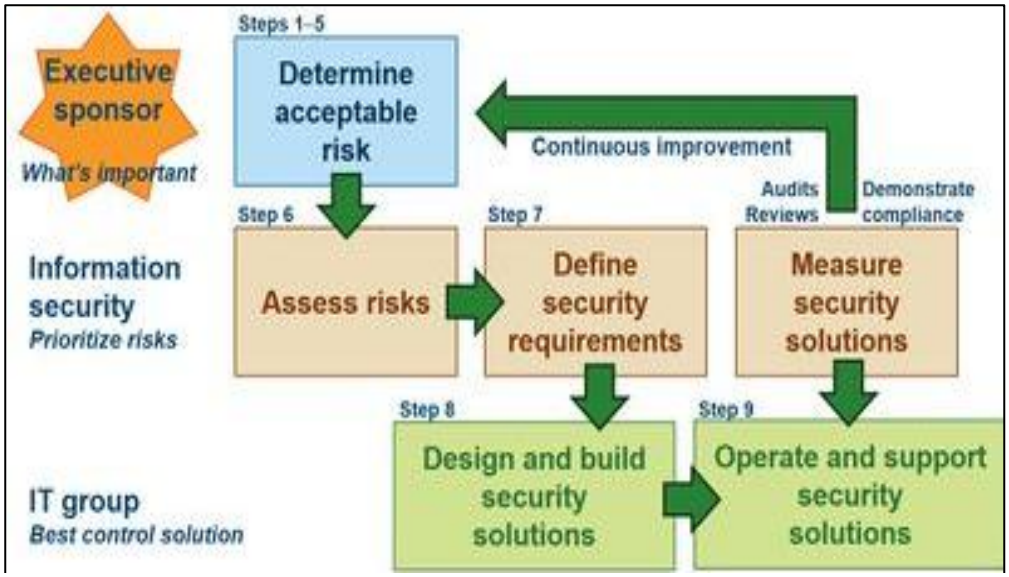

Fig. 5. Diagram of the security risk management process
Source: http://wiki.gis.com/wiki/index.php/Information_Security

Standard approaches to security risk management are well established and should be followed to ensure compliance (IEC/ISO 31010: 2009; He & Gong, 2009; Neves et al., 2015). The basic pillars of this approach with respect to GIS are in Figure 6.

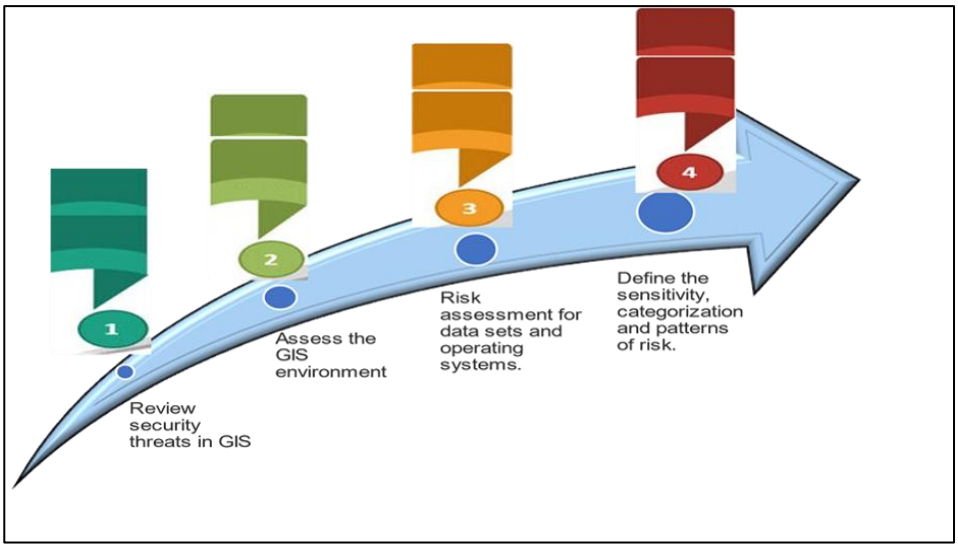

Fig. 6. Basic pillars of the standard approach
Source: The author's own elaboration

The key steps towards effective GIS information security are described in Table 1.

Table 1. Key steps towards effective GIS information security

Step name	Description
1. Legislation	Review regulations related to your industry. Security regulations can dictate compliance standards and security implementation frameworks; failure to comply can have negative business consequences.
2. Benefits	Identify any potential benefits to be gained from security compliance and operational savings attributable to the proposed security programme. This may be helpful in justifying the expenditure on the security programme.
3. Objectives	Set out the objectives of the SMART Information Security Programme. The objectives should be specific, measurable, achievable, relevant and time-bound.
4. Framework	Identify the information security management approach and methodology that will deliver results. Information security frameworks can be GIS-specific and share best practices that meet GIS business needs.
5. Approved planning	Establish a security risk assessment plan. You will need management authorisation for the required resources, support and financing.
6. Risk assessment and risk mitigation	Complete a risk assessment security needs analysis, identifying potential threats and associated mitigation strategies (Landquist et al., 2013).
7. Security features	Identify security procedures (rules) and technology (tools) to be implemented to meet identified security needs.
8. Training and awareness	Design and build validated security solutions. Implement training and awareness programmes to implement and enforce identified security practices.
9. Implementation	Operate and support security solutions. Monitor protection levels and measure compliance.

Source: The author's own elaboration

Risk management system model for GIS

For the purpose of this paper, the following definition of Risk Management System for GIS is adopted: "GIS Risk Management System (RMS) – a set of rules, principles, policies, processes, good practices, human resources and other measures relating to the risk analysis and review processes in GIS".

The GIS risk management system cannot be a creation detached from corporate reality, but must be an integral part of the organisation's management system (Kole et al., 2007). The basic components of a risk management system are:

- the strategy, which, together with the policy contained therein, sets the objectives, basic rules and a set of guidelines for risk management; it provides the basis for the development of detailed regulations and procedures;
- policy rules for risk management;
- internal regulations, rules and procedures that define the risk management process;
- the risk management structure that defines the levels of governance and the competencies and responsibilities of those involved in the risk management process;
- employees/personal resources involved in the risk management process (their qualifications);
- technical resources and IT support to the risk management process;
- management documentation;
- reporting documentation/system audit records;

In light of the above definition, an ordered five was adopted as the risk system model for controlling and maintaining an acceptable level of risk of the key elements of the technical architecture of the GIS platform:

$$\mathrm{SR} \equiv < C, SOO, \mathrm{OOO}, \mathrm{STR}, \mathrm{LCM}, \mathrm{FSC}, \mathrm{RF} > \quad (1)$$

where:

C – objective of the operation of the RMS defined on the subject of the action,

SOO – the subject of the operation of the EMS, which is the set of functional persons that make up the organisation's security service,

OOO – the object of operation of the GMS, which are the GIS objects in relation to which the required security level must be maintained,

STR – structure and attributes of a risk management system

LCM – life cycle model of risk management system

FSC – family of acceptable security configurations for the GIS technical infrastructure;

RF – reconfiguration function; this representation is determined at the IT design stage so that this representation can ensure that an acceptable level of risk is obtained. An acceptable level of risk can be achieved by generating an

appropriate functional configuration of GIS and security of GIS technical infrastructure from a set of acceptable solutions.

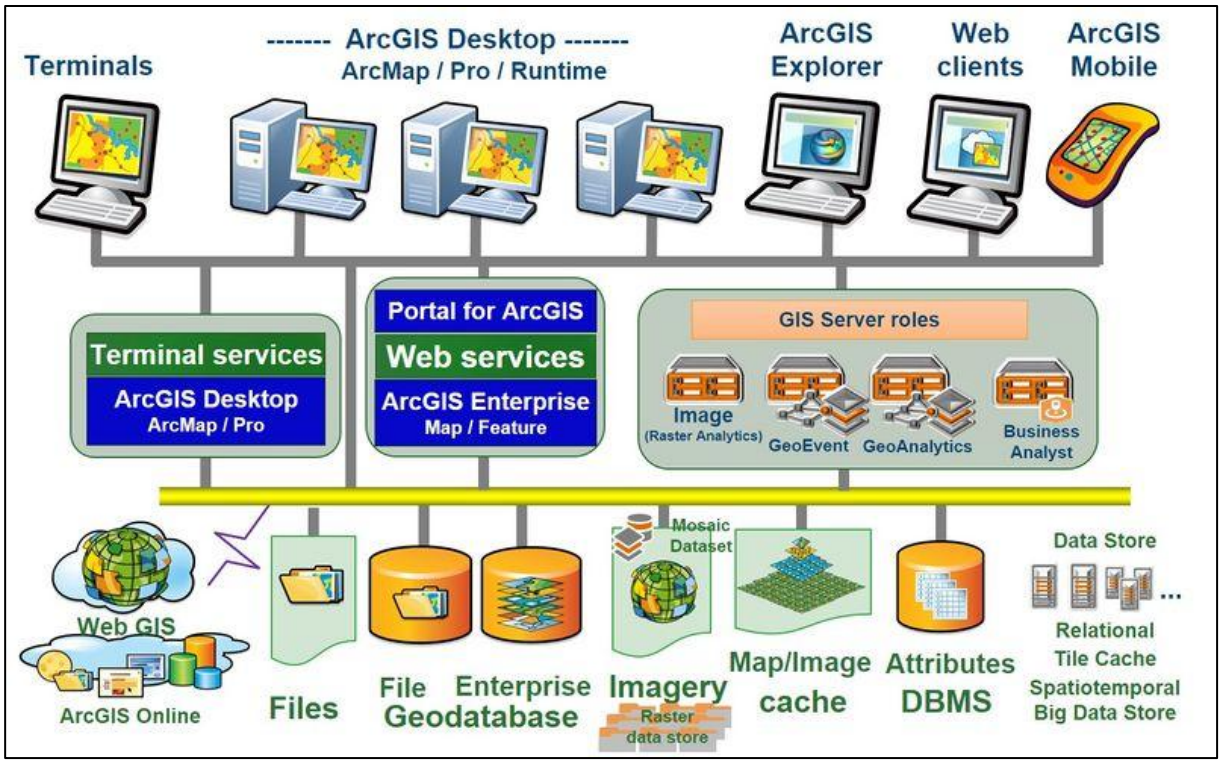

Fig. 7. Technical architecture of the GIS platform
Source: http://wiki.gis.com/wiki/index.php/Information_Security

The above elements shall be considered in the subsequent subchapters of this paper.

Subject of the operation. From the point of view of controlling the current level of information security, the subject of the operation may be:

- element of automatic development of control decisions, e.g. automatic security control system (ASCS),
- the set of functional persons, appointed within the project team and the security structure of an organisation's IT security management system (ITSMS), hereinafter referred to as the decision-maker.

Let`s introduce the following designations:

SF – set of ordered triples: $sf_p =< O_p, P_p, PO_p, MB_p > \in \Theta \times 2^P \times 2^{PO} \times 2^{MB}$, hereafter referred to as workstations; given the set of relations $\{R_i; i \in I\}$ defined on the set of SF, we can distinguish different functional structures of the GIS security service,

where:

Θ – the set of functional persons that may be nominated within the security service structure of the GIS; the set of these persons shall be defined at the stage of designing the GIS,

P – a set of protected resources owned by functional persons and for which they should maintain the required level of GIS security,

PO – a set of protective processes using appropriate protective methods and techniques of a technical or organisational nature, owned by functional persons of particular workstations; protective processes support processes of processing GIS information in the field of security and influence the continuity of business processes of the organisation.

MB – a set of security mechanisms at the disposal of functional persons and constituting

A set of controllable protective processes or protected facilities, or security mechanisms, or workstations shall specify the $\propto^{SB}$ purpose of the security service.

Object of the operation. From the point of view of controlling the current level of information security, GIS is the object of the operation of a set of such elements $e_j \in E^{GIS}$, GIS system, whose desired state may be determined by the decision-making entity (Stanik et al., 2018). The elements of the set E^{GIS} may be:

- Business processes or services;
- Organisational units;
- People;
- Locations;
- GIS IT infrastructure;
- GIS software and databases;
- Other documents and data (in electronic and other form).

Each resource of the GIS system shall be identified by a number $p \in P^{GIS}$ and described by a set of characteristics C_p^{GIS} names. If all different sets of features C_p^{GIS}, such as individual elements of the set E^{GIS}, are numbered with a variable $b = \overline{1,B}$ (which we call GIS resource type - object), then two objects are of the same type (e.g. 'b') when describing identical sets of characteristics. Sets of distinctive Q_p^{GIS} numbers describing the object $p \in P^{GIS}$ and the corresponding sets of distinctive names shall C_p^{GIS} not be empty for any person $p \in P^{GIS}$, where P^{GIS} it is a set of distinctive GIS resources numbers. We assume that for each feature $q \in Q^{GIS}$ a set A_q^{GIS} of possible performances a_q of the feature is defined.

Objective of operation of the risk management system. The operation of a risk management system can be defined:

1) with respect to the control of the security properties of GIS assets as an ordered pair:

$$DZ^{SIO} = <\propto^{SIO}, Z^{SIO}>, \tag{2}$$

where:

$\propto^{SIO}$ – the purpose of GIS in the context of information security,

Z^{SIO} – set of tasks for the secure processing of GIS information sets ensuring the achievement of the objective $\propto^{SIO}$.

2) with respect to the control of the performance features of the IT GIS infrastructure as an ordered pair:

$$DZ^{IT} = <\propto^{IT}, Z^{IT}>, \tag{3}$$

where:

$\propto^{IT}$ – the purpose of the GIS IT infrastructure,

Z^{IT} – the set of tasks (controls) of an IT administrator ensuring the achievement of a goal $\propto^{IT}$.

Structure and attributes of the risk management system. The Schematic illustration of the structure of the risk management system are shown in Figure 8.

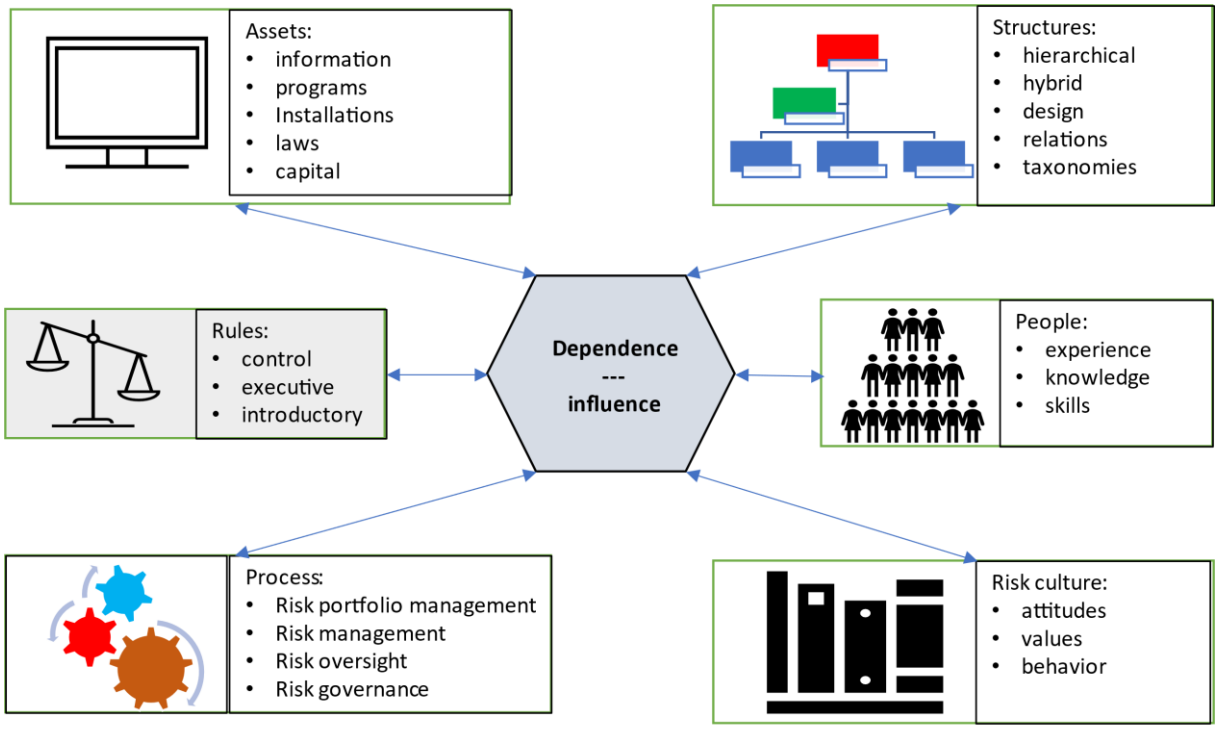

Fig. 8. Basic categories of risk management system components and their attributes
Source: The author's own elaboration

Each of these components is important for proper and effective risk management. The importance of any of these elements cannot be overlooked. The elements (components) identified in this way remain among themselves in specific relationships and system dependencies, which enables them to fulfil the common mission for which the RMS was created:

$$RMS = < \mathrm{E}^{RMS}, R^{RMS} \subseteq \mathrm{E}^{RMS} \times E^{RMS} > \rightarrow \boldsymbol{U}^{RMS} \tag{4}$$

where:

RMS – Risk Management System,

E^{RMS} – the set of elements of a risk management system,

R^{RMS} – set of system relations,

$\boldsymbol{U}^{RMS}$ – the usability of a risk management system.

Risk management systems must be characterised by specific performance characteristics that determine, inter alia, attributes such as objectives, functions, purpose, scope, boundaries, environment, structure, maturity, functionality, reliability, innovation and continuity of operation, under specific environmental conditions. We assume that usability, as an imperative feature of a risk management system, is a composite function of individual usability attributes:

$$\boldsymbol{U}^{RMS} = f(w_i^{RMS} \in \mathbb{W}^{\mathrm{RMS}}; \mathrm{i} \in \mathbb{I}^{\mathrm{RMS}}) \tag{5}$$

where:

$\mathbb{W}^{\mathrm{RMS}}$ – a set of distinguished usefulness attributes of the risk management system,

w_i^{RMS} – i-th attribute of usefulness of the risk management system,

$\mathbb{I}^{\mathrm{RMS}}$ – a set of numbers of distinguished attributes of the risk management system.

Life cycle of risk management system. In the relevant literature it is very difficult to find a definition or concept of a life cycle model of risk management. Very often this term is associated with the concept of risk management in information security (Jajuga & Kuziak, 2006; Bhattacharya, 2015; Escanciano & Olmo, 2007).

The concept of the system life cycle should be understood as a specific concept of the distribution of stages, phases or activities over time. ISO 31000 includes specific regulations for the different stages of the life cycle of the risk management process**,** such as:

1. Communication and consultation as part of risk management;
2. Determining the internal and external context and the context of risk management;
3. Defining risk criteria;
4. Risk estimation, i.e. identification and analysis of threats and risk assessment;
5. Determining a risk management strategy taking into account the different degrees of effectiveness of these strategies;
6. Preparation and implementation of risk management plans;
7. Monitoring and reviewing;
8. Documenting the risk management process.

In this paper, with reference to GIS class systems, the authors propose the following phases of the risk management system life cycle (Fig. 9).

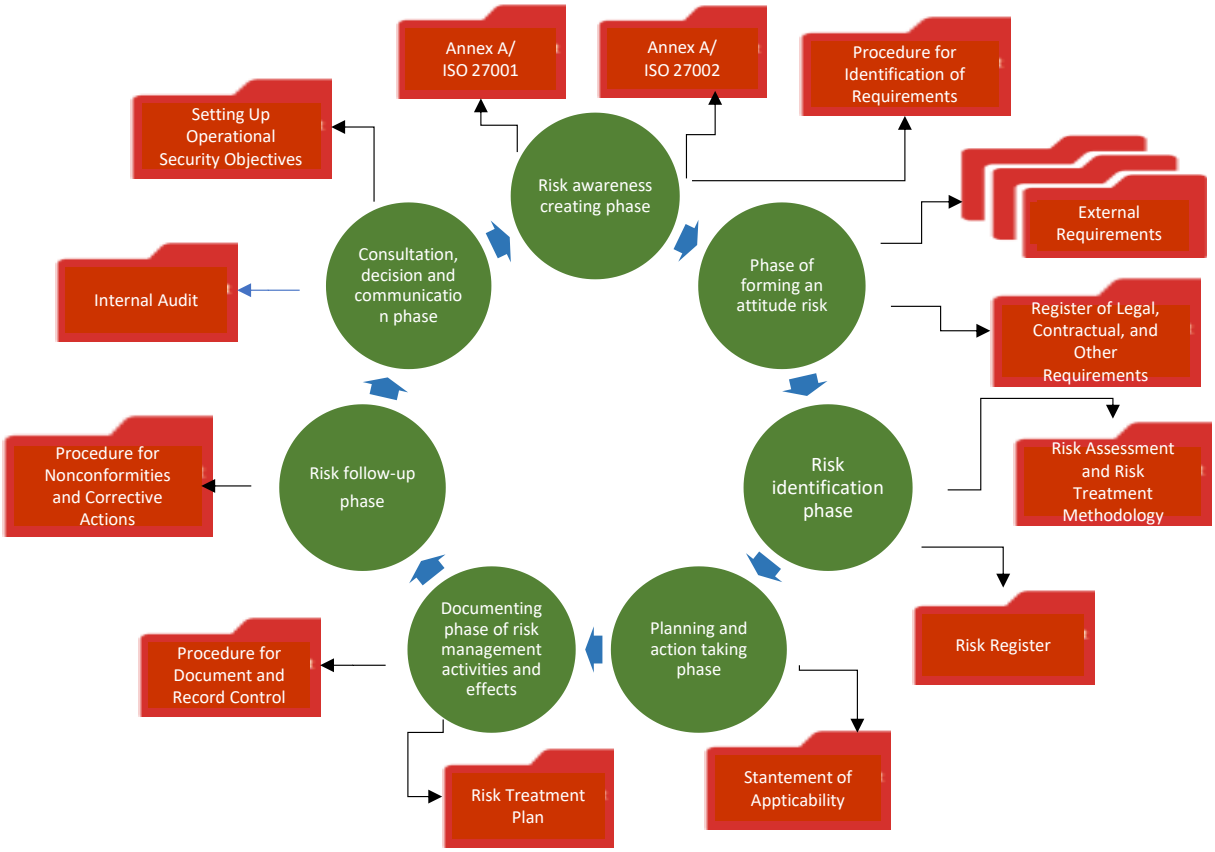

Fig. 9. Life cycle model of risk management system
Source: The author's own elaboration

Family of acceptable GIS infrastructure security configurations. Let's introduce the following notation of any security configuration:

$$KB_{kl} = \langle OB^{kl}, O^{k},\ MB^{l} \rangle \tag{6}$$

where:

- OB^{kl} – a set of information resources of the organisation's information system which such resources are protected by the security configuration,
- O^{k} – a set of functional persons involved in ensuring the security of information resources belonging to the set OB^{kl},
- MB^{l} – the set of security mechanisms of a technical or organisational nature that constitute the security configuration.

Knowledge of the security configuration KB_{kl} makes it possible to assign to each set OB^{kl}, with a fixed set MB^{l} of security mechanisms (organisational and technical safeguards), the corresponding set O^{k}. The security configuration KB_{kl} is feasible if and only if the set OB^{kl} with the fixed elements of the set MB^{l} can be assigned such *set* O^{k}, that will ensure that the required security level is maintained for the set of information resources OB^{kl}.

It is assumed that the GIS security team is equipped with a visualisation subsystem, an automatic security control subsystem and a control and diagnostic team capable of

identifying all types of GIS emergencies (security loss situations). The concept of an emergency situation $a \in A$ of type u shall $\in U$ be understood as the sets OB_n, O_m, MB_s remaining after the occurrence of an emergency situation with number u $\in U$.

The set of acceptable functional configurations after the occurrence of an emergency situation of number is determined based on knowledge (Stanik, 2019):

- OB^p – a set of GIS assets for which the required security level must be maintained,
- O^p – the set of human resources (functional persons) available after an emergency with the number u $\in U$,
- $MB^p \in$ MP – the set of deployable security configurations based on the sets of operable technical and organisational security safeguards remaining after a security loss of u $\in U$,

based on the following rule:

$$KB_{dop}^{u} = \begin{cases} \{KB_{kl} = \langle OB^{kl}, O^{k}, MB^{l} \rangle \in \Theta B_p \times \Theta_p \times MP_p : \\ OB^{kl} \supset OB^{p}\}, \ if \ \bigvee_{\langle k,l \rangle \in K^u \times L^u} (OB^{kl} \supseteq OB^{p}) . \\ \Phi \ \ in\ the\ opposite\ case\ -\ an\ empty\ set. \end{cases}$$

The above means that the set of KB_{dop}^{u} acceptable security configurations, after a loss of the ability to provide the required level of security to the GIS assets, includes all security configurations, built for different variants of personal sets and a set of safeguards of a technical or organisational nature, remaining after the occurrence of an emergency situation, which ensure that the required level of security is maintained for the current set of information assets $OB\ (t) \in \Theta\mathrm{B}(t)$. Each security configuration from the set KB_{dop}^{u} ensures that an acceptable level of security is maintained for the information resources from the set OB^{kl}.

FR mapping shall be determined at the design stage of the control system at the current level of security or at the establishment stage of the protection system, as an essential element of the SMS, to ensure that the desired objectives of the operation of the Security Service and of the information processing subsystem are achieved during their operation, despite an emergency situation. After an emergency situation – i.e. loss of the required level of security in order to effectively continue the process of safe processing of information in GIS, it is necessary to generate acceptable or optimal security configuration. Generation of the optimal or suboptimal security configuration, from among sets of permissible solutions is implemented on the basis of detailed reconfiguration function Q, which from the point of view of their essence is the criterion function.

Conclusion

Enterprise GIS environments cover a broad spectrum of technology integration. Most environments now include a variety of hardware vendor technologies, including database servers, storage area networks, Windows terminal servers, Web servers, map servers and desktop clients – all connected by a wide range of local area networks, wide

area networks and Internet communications. All these technologies must function properly to support a sustainable calculation environment and to ensure the effective functioning of cybersecurity in the GIS environment. Global cybersecurity of GIS is the accident of distinguished types of cybersecurity in the field – related to the distinguished categories of resources of information systems, types of cyber threats and elements of the technical architecture of GIS platform. Risk identification is a key step in the risk management process. The main contribution of these studies is to fill the research gap related to the lack of a proposal for a methodical, comprehensive approach to the development of an adequate GIS security model and risk management life cycle model for ISO 27001 certification. The additional value of this article is to use elements of good practice in dealing with risks that can enrich the process of drawing up the Application Declaration Document (SoA) – to make it more accurate.

This article shows that it is possible to create "good enough" GIS security models and a risk management system for GIS. The following conclusions arise from the considerations set out in this paper:

1. In order to eliminate the consequences of failure – maintaining the required level of reliability of the technical architecture of the GIS platform, security of IT resources and an acceptable level of risk, it is reasonable to clearly specify the following steps in the life cycle of the risk management system:
   - preparation of the Application Declaration Document (SoA),
   - determination on the basis of the SoA of a set of acceptable functional configurations in a given emergency situation,
   - determination of a set of acceptable protection configurations for a given emergency,
   - carry out the reconfiguration process in a given emergency.
2. The proposed way of controlling the current performance of the GIS platform technical architecture and the GIS security configuration should be an integral part of the risk management system.
3. Using the results of this work, it is advisable to conduct and develop further research in the following directions:
   - improvement of the GIS security model taking into account the guidelines of standards in the areas of reliability, security, cyber security and risk,
   - increase the precision of the proposed risk management system life cycle model by including more detailed parameters and variables.

This paper is not a ready-made recipe for comprehensive risk management in GIS class systems. This should only be regarded as a proposal by the authors for a partial solution to the problem.

References

Aranoff S. (1989). Geographic Information Systems: A Management Perspective, WDL Publications, Ottawa.

Bhattacharya J. (2015). Quality Risk Management – Understanding and control the risk in pharmaceutical manufacturing industry, International Journal of Pharmaceutical Science Invention, vol. 4 (1), pp. 29–4.

Escanciano J.C., Olmo J. (2007). Estimation Risk Effects on Backtesting for Parametric Value-at-Risk Models, Working Paper, http://papers.ssrn.com/sol3/papers.

Gregoriou G.N., Hoppe C.H, Wehn C.S. (2010). The Risk Modeling Evaluation Handbook: Rethinking Financial Risk Management Methodologies in the Global Capital Markets, McGraw-Hill, New York.

He X., Gong P. (2009). Measuring the coupled risk: A copula-based CVaR model, Journal of Computational and Applied Mathematics, vol. 223, pp. 1066–1080.

IEC/ISO 31010: 2009. Risk management – Risk assessment techniques, Geneva, ISO.

Jajuga K., Kuziak K. (2006). Model Risk Measurement – General Concept and Particular Models. In: Mathematical, Econometrical and Computational Methods in Finance and Insurance, ed. P. Chrzan, Wydawnictwo AE w Katowicach, Katowice, pp. 107–116.

Kole E., Koedijk K., Verbeek M. (2007). Selecting copula for risk management, Journal of Banking & Finance, vol. 31, pp. 2405–2423.

Landquist H., Hassellöv I.-M., Rosén L., Lindgren J.F., Dahllöf, I. (2013). Evaluating the needs of risk assessment methods of potentially polluting shipwrecks. Journal of Environmental Management, vol. 119, pp. 85–92.

Neves A.A.S., Pinardi N., Martins F., Janeiro J., Samaras A., Zodiatis G., De Dominicis M. (2015). Towards a common oil spill risk assessment framework – Adapting ISO 31000 and addressing uncertaintie.

Peggion M., Bernardini A., Masera M. (2008). Geographic information systems and risk assessment. Luxembourg: Office for Official Publications of the European Communities.

Sienkiewicz P. (2005). Teoria inżynierii bezpieczeństwa systemów, Monografia nr 3 (*Systems security engineering theory, Monograph No. 3*), Kraków, AGH.

Sienkiewicz P. (2013). Teoria efektywności systemów (*Systems efficiency theory*). Ossolineum, Wrocław.

Stanik J., Kiedrowicz M., Waszkowski R. (2018). Security and Risk as a Primary Feature of the Production Process, ISPEM 2018 (The Second International Conference on Intelligent Systems in Production Engineering and Maintenance).

Stanik J. (2019). The risk model of an it system that processes Spatial data in SIP/GIS. 26th Geographic Information Systems Conference and Exhibition GIS ODYSSEY 2019.

Wróblewski D. (ed.) (2015). Zarządzanie ryzykiem – przegląd wybranych metodyk (*Risk management – review of selected methodologies*), Józefów, Wydawnictwo CNBOP-PIB.