GIS Odyssey Journal

2021 • Volume 1 • Number 2

https://doi.org/10.57599/gisoj.2021.1.2.5

Jerzy Stanik[1], Maciej Kiedrowicz[2]

METHODS, TECHNIQUES AND TOOLS FOR IDENTIFYING AND VALUING GIS ASSETS FOR MEASURING SECURITY, QUALITY AND RISK

Abstract: This paper attempts to develop and characterize instruments and approaches to the problem of identification, protection and quality of information processed in GIS class systems. One of the issues that causes most problems in the process of identifying and valuing GIS resources for measuring security, quality and risk is the proper selection of methods, techniques and tools for collecting and compiling various types of data in relation to these resources. In the process of identifying and valuing GIS resources, there is no list of test methods and techniques "reserved" for GIS only. It uses all – quantitative, qualitative and mixed – approaches and methods used in various studies. When designing an appropriate set of methods, techniques and tools in the process of identifying and valuing GIS resources, it is also important to remember to collect only those data that are really necessary. Proposed methods, techniques and tools take into account all the features, characteristics and determinants of GIS resources necessary to measure their security, quality and risk. A set of GIS resource identification instruments has been proposed, the implementation of which will significantly contribute to an increase in the level of security, reliability and quality of these resources. The proposed elements of a set, which are theoretically justified, may be improved and the set may be extended to other elements of the security policy. Far-reaching flexibility is called for in the choice of methods, techniques and tools used to identify and value GIS resources.

Keywords: GIS, risk, information resource, security, quality

Received: 11 September 2021; accepted:20 October 2021

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

Introduction

The expanding range and functionality of GIS class systems, the diversity and scope of services and the increasing requirements and expectations of their users have led to the search for new solutions for collecting and transmitting various types of information resources, e.g. data, spatial information, knowledge, etc. At a time of the information society, efforts are being made to obtain both an efficient and efficient flow of these information resources. The market driven economy requires constant adaptation to customer needs, thus improving the internal infrastructure of GIS class systems. The quality, security, risk and temporal and spatial aspects of the services offered by these systems have become an extremely important factor. Therefore, along with technological developments, the position of the IT infrastructure of the GIS class systems in supporting the information society has been strengthened. Gradually, new solutions were introduced, ranging from automatic identification and communication technology to integrated quality, security and risk management.

There are a number of methods, techniques and tools for identifying GIS assets for measuring security, quality and risk, with some being less and others more versatile. In order to identify and classify these instruments (methods, techniques and tools), a bibliometric analysis was carried out, on the basis of which the dynamics of interest in this subject, manifested in the number of publications in the analysed period, was assessed. The publication was reviewed in the Scopus database. The database was selected due to its size and availability. The phrase included in the titles, abstracts and keywords, on the basis of which the database lookups were conducted, was "Methods and techniques of data identification in the field of information security". The lookup area has been limited to publications concerning the Information and IT security area. The last 10 years were analysed (2010–2020). During this period, approximately 1000 (exactly 988) studies registered in the database were created, the largest part of which were Papers 679 (70%), conference releases 211 (21.1%) and reviews 48 (4.8%).

During the analysed period (2010–2020), an increasing trend can be observed in the context of the number of studies on methods, techniques and tools for the identification of GIS resources for the measurement of security, quality and risk, related to this topic. A clear interest in the subject matter is evident throughout the time period covered by the survey. Such a large number of studies indicate that the emphasis on continuous improvement of security and the need to deepen awareness of these issues is constantly increasing.

This study analyses and presents those methods, techniques and tools for the identification and identification of GIS resources for the purpose of measuring security, quality and risk, which are most often and widely used in practice. The selection of the methods, techniques and tools presented has been made on the basis of their frequency in publications and they are of the nature of good practices or standards.

It should also be noted that a well-selected identification system should meet, inter alia, the following criteria:

- should provide a cheap, reliable and ready for automatic recognition way to label products,
- should enable access to the necessary data at each stage of manufacture and distribution of products,
- should enable the transmission of data in a structured and comprehensible manner for all concerned.

Process for identifying GIS assets for measuring security, quality and risk

A schematic illustration of the GIS resource identification process for measuring security, quality and risk and its environment is shown in Figure 1.

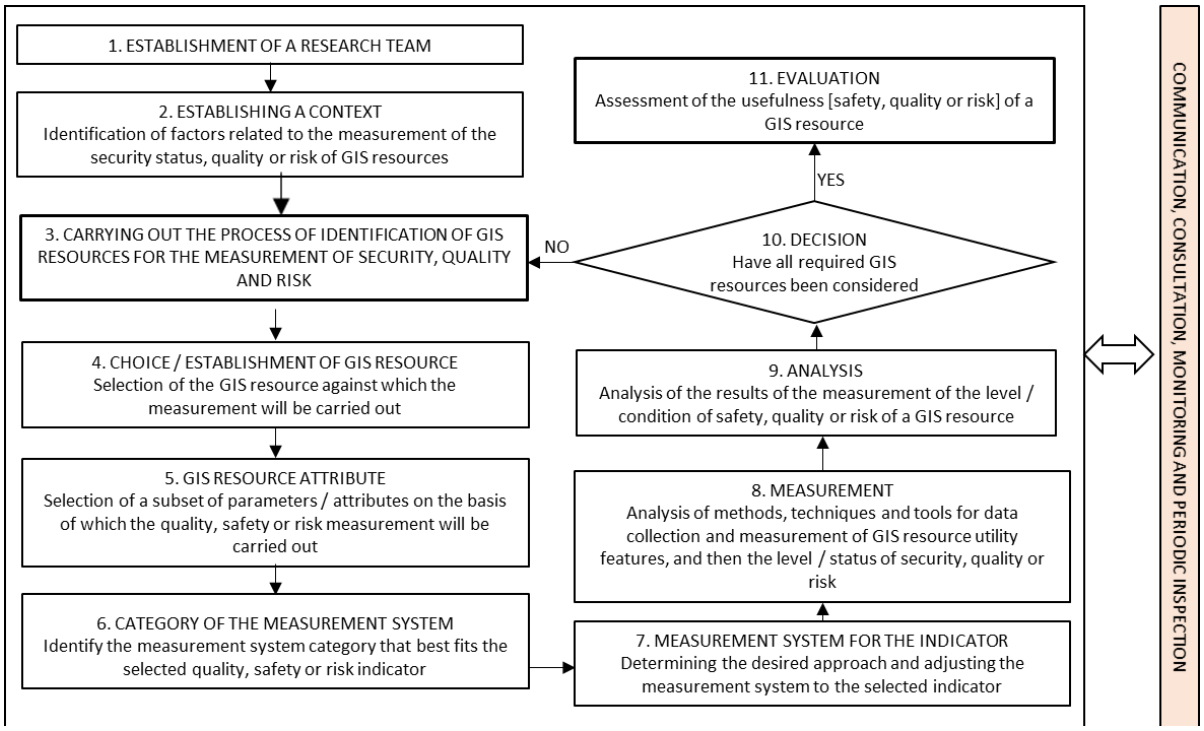

Fig. 1. Illustration of the process of identifying and valuing GIS resources for measuring security, quality and risk
Source: Own study

In this figure, four (colour-coded) important groups of elements are distinguished, comprising:

1. The GIS class system and its perspectives;
2. The process of identifying and valuing GIS resources for measuring security, quality and risk;
3. Risk analysis process for measuring the security or quality of GIS assets;
4. System for protecting/securing GIS sensitive resources.

The first step in the process of identifying and valuing GIS assets for measuring security, quality and risk is to establish the context. The second stage focuses on the identification of sets of information packets/resources residing on various information media, e.g.: paper, electronics, human brain, and consists of two specific steps:

1. Automatic identification aimed at automatically collecting, storing or entering descriptions of GIS information resources into the database of the computer system, i.e. referring to automatic identification. In literature, terms such as AI (Automatic Identification), Auto - ID (Automatic Identification) or ADC (Automatic Data Capture) may be met. The diversity of names used in this case results from the continuous development of IT technology and thus improvements and modifications aimed at improving and classifying the methods used (Jedynak & Bąk, 2917; Stanik & Kiedrowicz, 2018; Kwaśniowski & Zając, 2004; Lejuez et al, 2002).
2. Traditional identification aimed at determining the actual status of sets of information packets residing on electronic media at a given moment, verifying their usefulness, valuing and comparing them with records, settling and clarifying differences, settling persons materially responsible for sets of information packages, and finally adjusting records to reflect an actual state.

The third step, after identification, is the acquisition, collection, archiving, analysis and presentation of data. It may be disaggregated into the following phases:

- obtaining spatial data,
- collecting data in an automatic way,
- archiving information assets,
- analysing, presenting or visualizing data.

The next step, once the asset identification has been carried out, is to agree on a scale and criteria for assigning all assets a specific place on the scale, based on asset valuation. Given the variety of assets operating in GIS, it is likely that some assets can be assigned a specific value expressed in money, while for others a range of values can be indicated only, for example, from “very low” to “very high”. The decision to use a quantitative or qualitative scale depends on the organization’s preferences, but it is recommended to refer to assets. Both types of valuations can be used for the same assets.

Typical terms used for the qualitative valuation of assets are: negligible, very low, low, medium, high, very high and critical. The choice and scope of terms suitable for GIS depends to a large extent on needs for the security, quality and size of GIS and other factors specific to a given GIS class.

The fifth stage focuses on the protection of GIS information packages residing on various information media, in particular on electronic information carriers, and the following processes/areas can be distinguished:

- protection of sets of information packets sent in the GIS computer network,
- protection of access to sets (resources) of information packets.

The entire process of identifying GIS assets for security, quality and risk measurement is iterative and is supported by communication, consultation, monitoring and periodic review (Allen et al, 2018; Suchecka & Nieszporska, 2015). Sets of methods and techniques for identifying GIS resources, for measuring security, quality and risk, are presented in Table 1.

Table 1. Methods and techniques for identifying GIS resources, for measuring security, quality and risk

Name of process step	Groups/types of methods, techniques and tools	Identification	Valuation	Characteristics of the method/technique/tool
E1. Establishing the context.	E1.1. A systems or process approach. E1.2. An iterative approach.	–	–	Depending on the scope and purpose of the GIS, different approaches may be used. The approach may also be different for any iteration. It is recommended to select or develop an appropriate approach to security, quality or risk management relating to basic criteria such as risk assessment criteria, security and quality assessment criteria, consequence criteria, risk acceptance criteria.
E2. Identification of GIS resources	E2.1. Inventory of information packets	–	–	List by nature of the number of sets of information packets, valuation of those quantities, comparison of the values received with reference data or electronic repositories, including databases or data warehouses, and explanation and settlement of possible differences.
	E2.2. Global EAN UCC identification system	+	++	A consistent approach to identification and communication, thus aiming to create and develop a common language for the wider business. The EAN UCC system includes identification data that can be applied to various facilities, including information resources, following their coding in specific bar codes.
	E2.3. Automatic Data Capture (ADC) and storage or Automatic Identification (Auto ID) systems.	++	++	They enable the processing of information in electronic form, which helps to manage available resources more efficiently, including collections of information packets transferred on electronic media. With regard to sets of information packets residing on electronic information media, automatic identification can be performed with using (Robinson, 2016): - Bar code, - Radio Frequency Identification – RFID, - Magnetic strip, - Optical Character Recognition – OCR, - Visio system, - voice solutions.
	E2.4. RFID technology	++	+	It is among the fastest growing automatic identification techniques. Its development results both from the continuous improvement of the efficiency of the technology itself and from the reduction of the costs of its implementation and the introduction of global standards. However, it is perceived as threatening civil liberties.
	E2.5. Radio Frequency Identification System RFID – Electronic Product Code (EPC) – RFID identification standard - EPC global – Image recognition systems – Biometric technologies	+	+	Radio Frequency Identification (RFID) technology has greater capabilities than bar codes and enables their disadvantages to be eliminated. By using radio waves and electronic labels, it is possible to detect and identify objects from a long distance, regardless of the position and visibility of the label with the reader. The RFID identification system consists of transponders (tags) and readers together with control devices and data transfer devices. Transponders can be designed as Read Only devices (Read Only – writing is done during production - limitations similar to bar codes), as Write Once Read Many times (WORM) devices, or as devices that are able to write and read data repeatedly.

E3. Data collection, archiving, analysis and presentation	E3.1. Automatic data collection methods (Robinson, 2016):			Automatic identification is a complex concept, applies both to recognition, verification and identification processes. This complexity is due to the situation and the relationship between the identifier, the automatic reader, the database and the executive device. These relationships are determined by the choice of a specific automatic identification technique, which, if properly selected for a given GIS, enables to increase the efficiency of the business activities undertaken.
	– optical	+	–	They enable recognition of the presented image and optical recognition of graphic characters, letters, print, writing or coded structures. These include methods such as: OMR (Optical Mark Reading), OCR (Optical Character Reading), ICR (Intelligent Mark Reading), VS Image Recognition Systems (Vision Systems) and bar code techniques.
	– magnetic	+	–	They are based on the recognition of information recorded in the form of magnetic dots and dashes on a magnetic track. With the help of a magnetic reader, a reading is made which is possible even if the characters are blurred or crossed out. Magnetic methods are used for identification and authorization control, which is carried out on the basis of various types of magnetic cards.
	– electromagnetic	+	–	They are based on radio frequency identification with using an RFID system. These are wireless methods, reading is done in a non-contact manner. They enable identification and transmission of data over long distances, as well as remote saving and modification of information. By means of an antenna, a transmitter (receiver with a decoder) and a transponder (radiolocation device), the radio pulse is received and processed together with the information stored in it.
	– biometric	++	–	They allow identification of identity, based on fixed physical or behavioural characteristics (behavioural identification). The digitally encoded profile of the person is stored in the database or is on the personal card. The characteristics shall be written by means of a magnetic stripe or a two-dimensional bar code. 8 Identification may be based on physical characteristics such as fingerprint pattern, shape, proportions and dimensions of hands or fingers, pattern of blood vessels on the retina or characteristic points of the iris, facial features including the eye area, thermal image of the face and voice
	– tactile	–	–	Devices also known as contact devices, enable data to be read and entered by using a special probe. These are micro-devices in the form of stainless steel containers with an internal electronic memory chip. The upper part of the device is connected to one end of the electronic circuit, while the lower part, along with the sides, acts as an electrical mass. The whole circuit is closed by a probe.
	– smart cards	–	–	They belong to cards equipped with memory and a microprocessor. It is used to control, read and record information and manages the card memory by indicating its specific areas for recording selected data. Microprocessor cards have Read Only Memory, in which the operating system is stored. The operating system enables the microprocessor to function. There are many different models of smart cards. Some have their own battery power supply, e.g. Active Cards, others, equipped with a keyboard and display, are self-sufficient systems, e.g. Super Smart Cards. Smart cards include cryptographic cards (with embedded encryption accelerator, thus increasing data protection effectiveness), hybrid cards (using various technologies combining magnetic or optical cards with an electronic system) and cards with a dual interface (communication is possible through a radio interface or connector).

	E3.2. Systems for data archiving, analysis and presentation (Robinson, 2016):			These systems are an intermediate element between the GIS hardware layer and the business layer. It may include a geo-database responsible for efficient real-time archiving of often large amounts of data and various types of tools for processing and analysing this data, often based on artificial intelligence methods.
	- Historian industrial databases	+	–	Plant-wide Historian databases have an architecture aimed at collecting and presenting data being processed. They have a variety of built-in capabilities to collect processed data from multiple sensors and systems that operate in real time, producing huge data sets. Typically, the Historian system elements responsible for collecting various types of data are built as so-called collectors, ready for use immediately after installation. Data sources can be the industrial-standard OPC servers, but it is also possible to download data from other sources such as HMI/SCADA software from various manufacturers.
	- MES systems	+	–	MES systems are responsible for analysing and presenting spatial data collected in the Historian database and other sources. In order to enable them to function properly, it is necessary to build a correct data model taking into account the links existing therein.
E4. Valuation of resources	E4.1 Generalized method	++	++	The valuation of GIS resources is carried out in two (or more) iterations. The first one is an overall valuation carried out to identify potentially sensitive resources that open up the possibility of further valuation. The next iteration includes further, more detailed considerations on potentially high losses disclosed in the initial iteration. If it does not provide sufficient information to estimate the level of security, a further detailed analysis shall be carried out, presumably for a part of the overall scope, and possibly by using another method.
	E4.2. Detailed methods	++	++	The methods for the detailed valuation of resources in the GIS information security include the in-depth identification and valuation of GIS assets, the estimation of threats to these assets and the estimation of vulnerabilities. The results of these activities are then used to estimate the risks and then to measure the level of security or quality status. To evaluate assets/information resources by using the detailed method, functionals are used, described by the following formulations: $$F^a : AB \times KA \longrightarrow S^J \ , \ F^a(b_i, k_j) = f^a_{i,j} \in S^J$$ where: A – a set of assets, AB – set of basic security attributes, KA – a set of financial and non-financial criteria for assets, S^J – a scale of possible values of an asset

E5. Protection of GIS information packets	E5.1. Protection of sets of information packets transmitted over a GIS data communication network,	+	–	As regards the protection of information transmitted over the GIS network, it is essential to prevent the flow of unauthorized data and to define very strictly which data can be accessed and for what purposes, and which data are necessarily open and which are restricted. The protection of sets of information packets in open systems consists in/is implemented with using the following services (Stanik et al, 2014): – access control/controlling an access – protects resources against unauthorized users – confidentiality of data – a service designed to protect information or data against unauthorized persons – data integrity – data protection against data modification / erasure, i.e. it is cohesion security – authentication – control / security, identity of parties or data – non-repudiation – this is a control regarding the sending of information as well as the receiving of information – encryption – this involves making information secret, two encryption algorithms are distinguished: symmetric (with secret keys) asymmetric (with secret keys and public keys) – a digital signature – for which signing and verification procedures are defined; the former uses the input of information that is unique and confidential to the signatory, the latter uses information that is publicly available – access control – has been established in order to define and respect access rights – ensuring data integrity – the most common domain referred to as cryptography, i.e. control sums, is used in this case – authentication exchange – this is important for party authentication Three parameters are used here: challenges, time stamps, subsequent numbers – filling in with traffic – it hides information about the activity of a given source
	E5.2. Protection of access to sets (resources) of information packets.			In this respect, the following methods may be used: methods based on the control of the number of a responses set, methods based on the transformation (distortion) of responses or values of attributes of the information packets, methods based on making sets of information packets secret.

E5. Protection of GIS information packets	a) The method based on the control of the number of a responses set	+	–	This method is extremely simple, very easy to implement, and places a negligible burden on the time of usage (GIS information packet analysis) of a set of packets, and does not allow them to be accessed if they have been analysed on a smaller set of responses than it results from the time of access policy established for this set.
	b) Method based on transformation (distortion) of response	+	–	This method is among the most interesting because of its simplicity and at the same time high efficiency, especially when intrusives have additional external knowledge. To the greatest extent, it counteracts attacks with the use of spools.
	c) Cryptographic method - a method of making sets of information packets secret.	+	–	In cryptographic protection, a system is considered correct only if each attempt to "break" it forces to scan the entire space of contained keys, or if the time and complexity of such a scanning is equal to the time of such a review. It can therefore be said that the system becomes secure when it is correct and when a successful attack takes more time than the required period of classification of encrypted information.
	Techniques to protect sets of information packets collected in databases.	+	–	This is a problem that takes a great deal of attention and a variety of solutions, often very complicated, depending on protection requirements, are being taken in this regard. Despite the passage of several decades, the Denning's proposed division of data protection mechanisms in GIS databases into control mechanisms, such as the below mentioned ones, is still valid: - access control mechanism, - flow control mechanism, - control mechanism for data encryption and data inference (Denning, 1982; Denning, 1992). By limiting the scope of considerations, it can be noted that encryption, as the oldest technique for data confidentiality protection, has been developed outside IT, mainly by mathematics and communication specialists. From the point of view of IT systems, including database systems, it is primarily a technical problem consisting in the search for efficient implementation of theoretically recognized encryption methods. It is also worth noting that this technique prevents or significantly impedes the disclosure of the content of the information, but does not prevent any distortion or destruction of the data at all and can therefore only be used in databases as a complementary technique.

Legend: ++ – definitely applicable, + – applicable; – – not applicable

Source: Own study

The above groups of methods, techniques and tools for identifying GIS resources for the purposes of measuring security, quality and risk are only a reference point for those responsible for the management and administration of GIS resources. There is no algorithm advice on how to conduct the security, quality or risk measurement process for GIS resources. A more methodological approach to the problem is presented by (Fedulova & Lanovska, 2018). The authors use a mix of "top-down" and "bottom-up" strategies as complementary actions. Fedulova and Lanovska (2018) propose a list of questions useful to identify the symptoms and causes of the risk, risk factors, the risk situation and its consequences. In addition, the proposed list of questions concerns the method for detecting a specific source of risk. However, this approach is very general. Another methodological approach to risk identification is proposed by (Dzięcioł, 2018). This proposal is called the multidimensional risk analysis in the company. Despite the methodical level of the above-mentioned proposals, the methods do not answer

the question of how to perform comprehensive risk identification throughout the enterprise. One may wonder, in the context of the literature, this process should be characterized not only by "methodology" (Jedynak & Bąk, 20017), but also by multi- and inter-disciplinarily (Zawiła-Niedźwiecki, 2018).

Research methodology

The research presented in this paper is conceptual. This determines the lack of a research hypothesis. Nevertheless, this paper assumes that the process of identifying and valuing GIS assets for the purpose of measuring security, quality and risk will be successful (accurate) provided that GIS assets/resources are correctly disaggregated into basic ones and support ones and provided that values of possible damages/losses in case of loss of the security or quality attributes assigned to them, are correctly assigned/calculated to them. The basic research process led first to the development of a security, quality or information resource risk measurement model and then to the development of a methodology for measuring the security status of the GIS system or its information resources. The methodology takes into account groups of GIS resources and their attributes which, in the opinion of the members of the problematic/research team, allow a relatively objective and accurate assessment of the level of security, quality or risk of information resources. Due to the fact that individual factors or features of GIS resource usability within the distinguished areas of: quality, security and business continuity, belong to different sets of values, it is necessary to introduce a function ξ or a set of functions $\xi \epsilon \Xi$ unambiguously mapping these components to a uniform range of values.

The normalization function is referred to as the family of the functions $\xi \epsilon \Xi$ (Stanik & Kiedrowicz, 2018):

$$\xi : X \longrightarrow [1, 2, \ldots, N] \tag{1}$$

The form of the normalization function of the family Ξ should be defined in such a way as to represent their values in the range [1,..., N] and to maintain appropriate proportions of their impact on the overall usefulness of the GIS resource, taking into account the set X all specified utility factors. The set X should be decomposed into subsets X^B, X^J, X^C representing distinct areas/ /aspects.

The critical step in the GIS usefulness measurement process or a GIS security status is to determine:

- what is to be measured? (e.g. people, processes, activities, threats, policies, procedures, documentation, technical resources or other elements of the Armed Forces of Poland);
- what attributes, properties or utility features will be taken into account? (e.g. security, business continuity, etc.);
- how will the data be collected?;
- what data collection techniques will be used? (e.g. testing, research, interviews, observations, instruments, combined methods);

- what type of measures are best suited to selected elements and usefulness attributes? (i.e. binary measures, categories, structured measurements, measurements of factors, interval measurements);
- what category of measurement system is best suited to a given measurement situation? (e.g. descriptive, threshold or trend category);
- what measurement system and/or measure is the best to be used? (e.g. Likert's scale, binary measure, quotient measure, interval measure).

Having defined and determined a generalized GIS utility level based on a function F^{GIS} (a general GIS utility function determined on a set $\{A\}$ - the set of GIS utility parameters) we can finally introduce a definition of a partial GIS utility, e.g. F^B „ which represents the security aspect, and determine the GIS security level. Partial usability is related to a specific usability attribute and reflects its "contribution" to the total usability of the GIS system. The partial usability or usefulness of an attribute A_i is called a number $R_i \in$ R equal to the length of the vector.

Research findings

Model to measure security, quality or risk of information resource. In the literature of the subject matter and in available sources, in particular online resources (Laskowski, 2011; Bastien, 2009; Au et al, 2008; Fitzpatrick, 1998; Kuziak, 2006) several risk measurement models of any object can be found, ranging from simple models to developed and finishing on the most complex ones. These models have been presented in different ways, namely as:

- numerical models written by using mathematical formulae (Zikmund & Scott, 1977),
- graphic models written in the form of drawings, diagrams or constructed on the basis of Question aggregates (lists), or constructed on the basis of matrices, tables, maps,
- integrated models (combined, mixed) – resulting from a combination of numerical models or graphic models.

In this paper, the model for measuring the security, quality or risk of a GIS resource has been defined by the following formulation (Stanik & Kiedrowicz, 2018):

$$\text{MPBJR} =< Z, \{I\}, \{A\}, \text{F}^{GIS}, \{F^B, F^J, F^R\}, \text{MP} > \quad (2)$$

where:

Z – a set of key elements/information resources of GIS that are subject to identification and are the basis for determining their security, quality or risk status

$\{I\}$ – set of GIS resource identification instruments (it is a set of methods, techniques and tools necessary to identify GIS information resources)

$\{A\}$ – a set of GIS utility parameters (it is a set of basic GIS usefulness features disaggregated into three subsets $A^B \subset A, A^J \subset A, A^R \subset A$ of attributes, each of which reflects a subset of parameters enabling the measurement of quality, security or risk in relation to the established GIS resource)

F^{GIS} – the general GIS usability function determined on the set $\{A\}$

$\{F^B, F^J, F^R\}$ – detailed functions of usefulness of the information resource, properly determined on the subsets $A^B \subset A, A^J \subset A, A^R \subset A$

MP – methodology for measuring GIS usability or its components such as: quality, security, risk

Methodology for measuring the security, quality or risk status of the GIS information resource. Analysing the different approaches to measuring and handling the security, quality or risk status of a GIS information resource, the question arises whether it is possible to create a complete and coherent methodology taking into account the various internal and external factors relevant to the basic characteristics of GIS usability and linking them in a way that allows the level/status of security or quality to be determined as fully and unambiguously as possible, while maintaining the practical utility of the approach proposed.

This chapter is an attempt to answer such a question by presenting a description of the methodology for measuring the security, quality or risk status of the information resource, which, in the opinion of the authors, is a complete and consistent methodology (Figure 2).

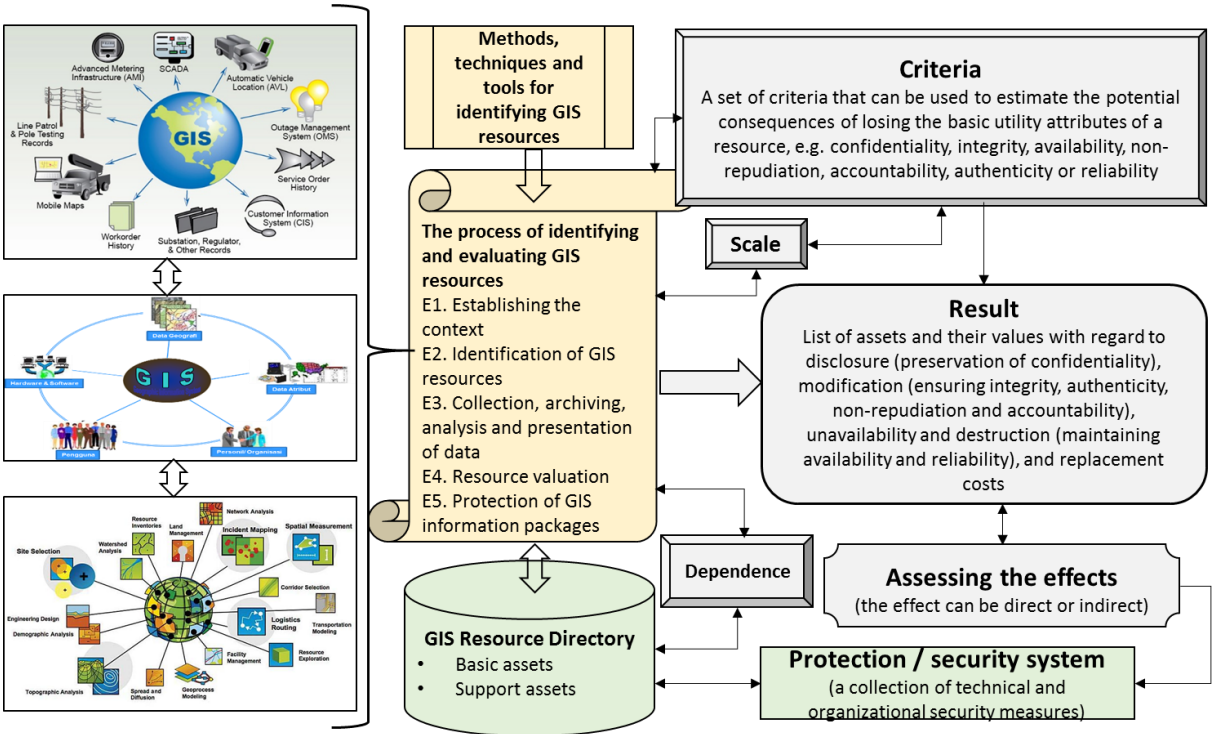

Fig. 2. Illustration of methodology for measuring the security, quality or risk status of the GIS information resource

Source: Own study

The basic elements of the methodology proposed in this paper are:

- A set of activities, conceived as stages or steps in a procedure and the links between them;
- A set of key GIS elements/resources that are measurable and form the basis for determining security, quality or risk status;
- A set of methods, techniques and tools for identifying GIS resources for measuring security, quality and risk;
- Set of attributes/properties of GIS usability, e.g. security, quality, risk;
- A set of indicators used to measure the characteristics of GIS resources and attributes of its resources, e.g. confidentiality, availability, integrity, reliability, accountability;
- A set of categories of measurement systems used to quantify security, quality or risk status;
- A set of types of measures used to express security, quality or risk status, e.g. binary measure, Likert scale;
- A set of data collection techniques, e.g. observations.

The starting point for establishing a methodology for measuring the security, quality or risk status of a GIS information resource is to select a leader or leaders to initiate the work, promote and coordinate the introduction of the programme, ensure effective communication and generally oversee the implementation of the programme. This function may be performed by one person or group of persons, depending on the size and complexity of the GIS or organization and the availability of personal resources. The team leader/team manager should plan the composition and structure of the measurement team. The structure of the team should be supplemented with roles (usually persons, groups of persons) which will represent all stakeholders. The respective roles will be assigned appropriate responsibilities appropriate to the tasks performed.

The determination of measurement systems and measures of the security, quality or risk status of a GIS information resource should start with establishing the context for a GIS operation in order to:

a) become acquainted with issues directly related to the structure and status of the GIS use environment and the elements/objects to be analysed and assessed in terms of security and quality,
b) identify internal and external factors related to GIS usability attributes,
c) lay down the basic criteria needed for measuring the security, quality or risk status of the GIS information resource:
   - criteria for selecting a set of indicators,
   - criteria for the selection of categories of measurement systems used to quantify the security, quality or risk status of the GIS information resource, criteria for the selection of data collection techniques,
   - criteria for selecting types of measures,
d) define the sets of key GIS resources,

e) define a set of attributes describing the usability of GIS,
f) define sets of measurement systems for established indicators to measure the security, quality or risk status of the GIS information resource, establish data collection techniques,
g) define categories of measurement levels – a set of measures.

Conclusions

One of the issues that causes most problems in the process of identifying and valuing GIS resources for measuring security, quality and risk is the proper selection of methods, techniques and tools for collecting and compiling various types of data in relation to various types of GIS assets. In the process of identifying GIS resources, there is no list of research techniques, tools and methods "reserved" only for it. The main contribution of these studies is to fill the research gap associated with the absence of proposal, of a methodological, comprehensive approach to the implementation of this phase throughout the security, quality or risk management process. An additional value of this paper is the development of a model and a method for measuring GIS usability that can enrich the risk management process (make it more accurate). This is reflected in the methodology presented. The methodology proposed in this paper has theoretical background but is aimed at practitioners. The methodology is universal and can be used in all types of GIS systems as part of a risk, quality or security management process. However, it is important that the choice of specific methods, techniques and tools to support the identification process at individual stages depends on the situation (e.g. nature, destination or size) and the capacity to analysing GIS and the range of needs.

The methods proposed in this paper for identifying and valuing GIS resources are quantitative, qualitative and mixed methods and can be applied to a variety of studies. The article also does not present a ready-made "canon" of methods and techniques that work in every situation with regard to the exploitation of GIS resources. It is often recommended to use, where possible, rather simple, "respondent-friendly" techniques and tools that do not require labour-intensive statistical analyses when developing the results collected. When designing an appropriate set of methods, techniques and tools in the process of identifying and valuing GIS resources, it is also important to remember to collect only those data that are really necessary. This paper attempts to develop and characterize instruments and approaches to the problem of identification, protection and quality of information processed in GIS class systems. Proposed methods, techniques and tools take into account all the features, characteristics and determinants of GIS resources necessary to measure their security, quality and risk. A set of GIS resource identification instruments has been proposed, the implementation of which will significantly contribute to an increase in the level of security, reliability and quality of these resources. The proposed elements of a set, which are theoretically justified, may be improved and the set may be extended to other elements of the security policy. Far-reaching flexibility is called for in the choice of methods, techniques and tools used to identify GIS resources. In the context of the studies carried out, it can be concluded that:

- The process of identifying and valuing GIS assets for measuring security, quality and risk resembles a research process, which is opened by a problem-solving team responsible for its progress, based on substantive and methodological knowledge (which such knowledge is often interdisciplinary). On the other hand, however, this fact sets out a duty of care and a high level of self-awareness of its "researcher".
- Identification of risk factors for the entire GIS from several different perspectives may reveal more sources of risk or challenges, and consequently the cognitive gap (the area of risk omitted) is limited to the minimum.

The most important limitation of the model and methodology for measuring the security, quality or risk status of a GIS information resource is the theoretical nature of their foundations. Further empirical research (e.g. case studies) is therefore recommended, as well as a theoretical critique of the model and methodology.

References

Allen B.J., Loyear R., Noakes-Fry K. (2018). Enterprise Security Risk Management: Concepts and Applications. Connecticut, Publisher: Rothstein.

Au F., Baker S., Warren I., Dobbie G., (2008). Automated usability testing framework. In: Proceedings of the Ninth Conference on Australasian User Interface, AUIC 2008, vol. 76, pp. 55–64.

Bastien J. (2009). Usability testing: a review of some methodological and technical aspects of the method. International Journal of Medical Informatics, no. 79(4), pp. 18–23.

Denning D. (1982). Cryptography and Data Security. USA, Addison-Wesley.

Denning D. (1992). Kryptografia i ochrona danych (*Cryptography and Data Security*). Warsaw, Publisher: Wydawnictwo Naukowo-Techniczne.

Dzięcioł P. (2018). Proces wielowymiarowej analizy ryzyka w przedsiębiorstwie (*The process of multidimensional risk analysis in an enterprise*). In: Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu, no. 541, pp. 19–38.

Fedulova I., Lanovska H. (2018). Identyfikacja ryzyka: Esencja i metody wykrywania (*Risk identification: Essence and detection methods*). In: Scientific articles Mykolo Romerio universitetas, no. 21, pp. 40–53.

Fitzpatrick R. (1998). Strategies for Evaluating Software Usability. Methods, vol. 353, no. 1, Publisher: Technological University Dublin.

Jedynak P., Bąk S. (2017). Przegląd standardów zarządzania ryzykiem (*Review of risk management standards*). In: E. Skrzypek, A. Piasecka, S. Sagan (ed.), Nowa jakość a zadowolenie interesariuszy (*New quality and stakeholder satisfaction*), pp. 49–68. Lublin, Publisher: Katedra Zarządzania Jakością i Wiedzą, Wydział Ekonomiczny UMCS w Lublinie.

Kuziak K. (2006). Metody analizy ryzyka operacyjnego (*Methods of operational risk analysis*). Prace Naukowe Akademii Ekonomicznej we Wrocławiu, no. 1133, pp. 254–265.

Kwaśniowski S., Zając P. (2004). Automatyczna identyfikacja w systemach logistycznych (*Automatic identification in logistic systems*). Publishing House of the Wrocław University of Technology, Wrocław.

Laskowski M. (2011). Czynniki zwiększające jakość użytkową interfejsów aplikacji internetowych (*Factors increasing the usability of web application interfaces*). Logistyka, vol. 6, pp. 2191–2199.

Lejuez C.W., Read J.P., Kahler C.W., Richards J.B., Ramsey S.E., Stuart G.L., Strong D.R., Brown R.A. (2002). Evaluation of a behavioral measure of risk taking: The Balloon Analogue Risk Task (BART). Journal of Experimental Psychology: Applied, no. 8(2), pp. 75–84.

Robinson A. (2016). More advanced technology trends in logistics in 2016, http://cerasis.com/ [access: 28.08.2021].

Stanik J., Kiedrowicz M. (2018). An Information System Risk Model for the Risk Management System of an Organisation Processing Sensitive Data. Journal of Management and Finance, vol. 16, no. 3/1, pp. 207–227.

Stanik J., Protasowicki T., Kiedrowicz M. (2014). Wybrane aspekty standaryzacji w ochronie publicznych zasobów informacyjnych i świadczonych usług w kontekście społeczeństwa informacyjnego (*Selected aspects of standardization in the protection of public information resources and provided services in the context of the information society*). Zeszyty Naukowe Uniwersytetu Szczecińskiego – Ekonomiczne Problemy Usług, Szczecin, vol. 113, pp. 113–130.

Suchecka J., Nieszporska S. (2015). Koncepcja ryzyka w kontekście funkcji użyteczności (*The concept of risk in the context of the utility function*). Zeszyty Naukowe Politechniki Częstochowskiej Zarządzanie. Częstochowa, no. 19, pp. 103–115.

Zawiła-Niedźwiecki J. (2018). Od zarządzania ryzykiem operacyjnym do publicznego zarządzania kryzysowego. Wyzwania badawcze (*From operational risk management to public crisis management. Research challenges*). Kraków, Publisher: eduLibris.

Zikmund W.G., Scott J.E. (1977). An Investigation of the Role of Product Characteristics in Risk Perception. Review of Business and Economic Research, New Orleans, La, vol. 13(1), pp. 19–34.