Computers & Security 90 (2020) 101709

Contents lists available at ScienceDirect

Computers & Security

journal homepage: www.elsevier.com/locate/cose

# Information security assessment in public administration

Edyta Karolina Szczepaniuk[a], Hubert Szczepaniuk[b,*], Tomasz Rokicki[b], Bogdan Klepacki[b]

[a] Polish Air Force University, Dywizjonu 303 no. 35 ST., 08-521 Dęblin, Poland
[b] Warsaw University of Life Sciences WULS – SGGW, Nowoursynowska 166 ST., 02-787 Warsaw, Poland

ARTICLE INFO

*Article history:*
Received 23 July 2019
Revised 21 November 2019
Accepted 28 December 2019
Available online 30 December 2019

*Keywords:*
Information security
Cybersecurity
Public administration
Information security assessment
Information security management

ABSTRACT

The aim of the article is to characterise and assess information security management in units of public administration and to define recommended solutions facilitating an increase in the level of information security. The article is considered a theoretical-empirical research paper. The aim of theoretical research is to explain the basic terms related to information security management and to define conditions for the implementation of Information Security Management System (ISMS). Within the scope of theoretical considerations, source literature, legislation and reports are being referred to. In the years 2016-2019, empirical research has been conducted, which aim was to assess the efficiency of information security management in public administration offices. The evaluation of results of surveys was accompanied by an analysis of statistical relations between the researched variables, which enabled to define effects of European Union regulations on the delivery of information security in public administration. Results of the empirical data show that in the years 2016-2017, in public administration offices, certain problem areas in the aspect of information security management were present, which include, among others: lack of ISMS organisation, incomplete or outdated ISMS documentation, lack of regular risk analysis, lack of reviews, audits or controls, limited use of physical and technological protection measures, lack of training or professional development. In the years 2018-2019, European Union solutions, i.e. the GDPR Regulation and the NIS Directive, have affected the increase in the security level of information in public administration and have a significantly limited occurrence of identified irregularities. Results of the research enable to assume that the delivery of information security in public administration requires a systemic approach arising from the need for permanent improvement.



## 1. Introduction

Implementation of IT in most of the areas of activity of the state, the economy and the society, generates many opportunities regarding automation of management processes and increase in efficiency and quality of realized services. Simultaneously, the introduction of IT solutions in the public sector implies the necessity to provide security of the realised services. For this reason, within public administration institutions, the Information Security Management System (ISMS) is being implemented, which purpose is to provide security of information resources of an institution and to provide uninterrupted realisation of institution's mission. ISMS covers a set of planning and organisational undertakings and it is based on risk management of information threats which can have destructive effect on functioning of a public administration institution. Therefore, information security management in public administration affects the efficiency, reliability, and quality of the realised public tasks.

Analysis of problems related to global phenomena within field of the information environment of the state enables to perceive development trends of threats to information for the elements of critical infrastructure of the state (see e.g. WEF, 2019). Countries where public administration operates on the basis of new technologies, became sensitive regarding interference in information processes. Preventing threats and providing security of information constitutes a significant challenge, both for specific countries, as well as for international communities.

Many countries and organisations acknowledge the need to develop efficient solutions that facilitate an increase in information security level (see e.g. Janczewski and Caelli, 2015). In Poland, the National Interoperability Framework (Dz.U. [Journal of Laws] of 2012, item 526) have obliged entities in public finances sector to design, develop, establish, implement and improve an in-

* Corresponding author.
*E-mail addresses:* e.szczepaniuk@law.mil.pl (E.K. Szczepaniuk), hubert_szczepaniuk@sggw.pl (H. Szczepaniuk), tomasz_rokicki@sggw.pl (T. Rokicki), bogdan_klepacki@sggw.pl (B. Klepacki).

https://doi.org/10.1016/j.cose.2019.101709

formation security management system. The indicated obligations regarding information security management in public institutions were not reflected in practice multiple times, which is indicated in the results of scientific research (Szczepaniuk, 2016), analysis and reports, including the results of control presented by the Polish Supreme Audit Office (NIK, 2016). A symptom of changes in this aspect was the obligation to implement in the European Union member states the principles of the so-called General Data Protection Regulation (GDPR regulation) (O.J.EU L 119/1, 4.5.2016 2016), and the directive on measures to boost the overall level of cybersecurity of networks and IT systems in the European Union (NIS directive) (O.J. EU L 191/1, 19.7.2016 2016). In Poland, the European Union documents were implemented in form of passing, amongst others, the Personal Data Protection Act (Dz.U. [Journal of Laws] of 2018, item 1000) and the Act on the National Cybersecurity (Dz.U. [Journal of Laws] of 2018 item 1560). Implementation of the European Union solutions into Polish legal order resulted in increase in information security level and privacy protection. Legal acts of EU affected improvement of the organisation structure and security procedures (e.g. risk management procedure, information security audits). Moreover, the number of effective physical and technical protection measures have increased (e.g. access control mechanism, backup copies). A significant change also included regular training and improvement of personnel skills (e.g. personal data protection trainings). In some of the public administration institutions there are still many information threat vulnerabilities present. Moreover, the environment of threats is dynamically changing due to increase in range of advanced tools and attack techniques. The outlined context indicates a necessity to perform further research regarding information security in public administration in order to assess and improve the currently implemented solutions. Moreover, the research issues of this article also include the research priorities of the European Union in the aspect of cybersecurity (ENISA, 2017).

## 2. Research methodology

The subject of the research is the public administration institutions in Poland, in the context of processes of managing information security. The public administration constitutes a complex mega-system comprised of multiple subsystems (see e.g. Możdżeń-Marcinkowski, 2012). Functional and organisational complexity of public administration, regarding information security management, constitutes an interdisciplinary subject of research. The theoretical basis of the discussed issue originates in many academic fields, e.g. computer science, management and quality sciences, security sciences, legal theory.

The main goal of the research is to assess information security management in public administration entities in Poland and to indicate recommended solutions which would facilitate an increase of the level of security of information. Reaching the adopted goal required realisation of the following, theoretical in nature, detailed goals:

- defining information security in public administration;
- identification of information security threats in public administration institutions;
- explaining the essence of security management in public administration;
- defining conditions for the implementation of Information Security Management System.

The need to realise the above theoretical considerations within context of the adopted research goal is justified by the fact, that within source literature, the issue of information security management in public administration is often analysed in a manner which separates it from functioning of a public institution as an entirety. Theoretical foundations of information security management are aimed at indicating the fundamental problem in implementation of ISMS which is the lack of systemic approach that would include institution's mission and its aspect of providing proper quality of delivered services. Moreover, evaluation of information security management process utilising empirical research required adopting scientifically justified assessment criteria.

The research issue, presented in a general overview, expresses the complex and interdisciplinary nature of the object and the goal of the research. Due to this fact, a research model proper for systemic analysis has been adopted (see e.g. Sienkiewicz, 1995). The adopted methodological approach enables to research issues present across distant fields of knowledge and to analyse various phenomena in a holistic approach, in which it is presupposed that the reality is being perceived as whole and not as a collection of parts.

The choice of research methods and tools was determined by the adopted research process model. In the aspect of theoretical deliberation, the source literature, legislations and reports were referred to. Within the range of empirical research, a questionnaire-based survey was performed. Evaluation of results of the survey was followed by analysis of statistical relations between the evaluated variables, which were assessed using a Chi-squared test and C Pearson contingency coefficient.

The Chi-2 ($x^2$) test is a nonparametric statistical test which enables to indicate the presence of relations between examined variables. The formula of Chi-2 relation test is defined as follows (see e.g. Zibran, 2007):

$$x^2 = \sum_{j=1}^{k} \frac{\left(O_j - E_j\right)^2}{Ej} \tag{1}$$

key:
$x^2$ – Chi-2 relation test
$O_j$ – size observed for a given group
$E_j$ – size expected for a given group

The C Pearson contingency coefficient is a measure of the strength of the relation between evaluated variables, and it is calculated using the following formula (see e.g. Vogt and Johnson, 2015):

$$C = \sqrt{\frac{x^2}{x^2 + n}} \tag{2}$$

key:
$C$– C Pearson contingency coefficient
$x^2$ – Chi-2 relation test
$n$ – test sample size

## 3. Theoretical basis of information security management

### 3.1. Definition of information security in public administration

Source literature provides many definitions of information security. Adopting a specific interpretation requires referring to the general theory of security and system security theory. As a consequence of adopted determinations, it is reasonable to explain the essence of information security and to adopt a specific proposition of terminology clarifying specificity of information security in public administration.

Security category is a complex and multi-dimensional term, which is confirmed by a variety of typology and definitions available in source literature (see e.g. Brooks, 2009; Degaut, 2015; Stańczyk, 1996). When perceiving public administration in terms of a system, it is reasonable to interpret security from the point of

**Table 1**
Attributes of information security.

| No. | Attribute | Characteristics |
|---|---|---|
| 1 | confidentiality | Providing that access to information is restricted only for authorised users |
| 2 | integrity | Providing that information is preserved in its original form, except a situation when it is updated or erased by authorised personnel. |
| 3 | availability | Providing that information is available for authorised persons in the required time. |
| 4 | accountability | Related to unequivocal assigning a given range of actions to a specific user. |
| 5 | authentication | Providing that identity of a user or resource is as declared |

*Source:* Alhassan and Adjei-Quaye, 2017; Barczak and Sydoruk, 2003; Liderman, 2012.

view of systemic research. On the basis of systemic analysis, there are two predominant approaches (Sienkiewicz, 2010):

- system security understood as a property of a researched object, characterised with resistance toward the occurrence of dangerous situations (threats), while the focus is on the vulnerability regarding the occurrence of security incidents;
- system security defined in terms of ability to protect the internal values (resources) of an object against threats.

According to the above definition, security is perceived in terms of a feature of a given system, which conditions the system's reliability and operational efficiency in case of occurrence of a security incident. Therefore, term security should be considered in relation to possible threats.

One of the general system security models is the one developed by Clements, according to which, the interaction between threats and a researched object is defined. Let there be a set of all threats $Z = \{z_1, z_2, z_3, \ldots, z_n\}$ and a set of all objects $O = \{o_1, o_2, o_3, \ldots, o_n\}$. A set of all points which are vulnerable to attack, that is – system penetration paths, can be expressed with a Cartesian product $R \subseteq Z \times O$, which defines interactions between the identified threats and objects (Stokłosa et al., 2010). A given object may interact with multiple threats or a single threat may interact with multiple objects. Threat identification can largely minimise the risk of its occurrence, due to the fact, that it provides the possibility to implement adequate security measures.

The Clements model defines a security system with the following set (Hoffman, 1982; Stokłosa et al., 2010):

$$S = \{O, Z, B, R, P\} \tag{3}$$

key:

$O$ - set of objects at risk of threat,

$Z$ - set of threats,

$B$ - set of security measures (protections),

$R \subseteq Z \times O$ – set of penetration paths,

$P \subseteq Z \times B \times O$ - set of penetration paths protected against attack.

In the presented approach, a system is considered fully secured if for each attack-vulnerable point (penetration path) a security measure is provided. Public administration units are characterised with their own specificity, security measures, vulnerabilities, and the resulting risk. Therefore, in order to provide a sufficient organisation of a security system, it is necessary to identify, analyse, monitor, and improve specific elements of a system. Realisation of the adopted assumptions requires a systemic approach, due to the fact, that between elements of a system, a cause-effect, time varying relations occur.

Current deliberations suggest adopting the notion, that term information security refers to the ability to secure legally protected information against unauthorised interference, e.g. unauthorised disclosure, modification, erasing of information, or actions which disable possibility to process information. When referring these determinations to information security in public administration, it must be underlined, that the basic task of public sector institutions is realisation of public tasks both within the internal domain (e.g. providing services for citizens) and external domain (e.g. cooperation of public administration units). The functioning of public administration is based on gathering, processing and sharing information, therefore the information is one of the basic assets and it is considered a protected value. A security incident may significantly lower the quality of administrative service by disrupting the process of its providing. In extreme cases, it may result in disabling possibility to provide services by public administrations (Szczepaniuk, 2016). Information security in public administration is related to the ability to provide realisation of administrative processes and information security on every level of activity of public institutions.

Information security is often defined in the context of providing attributes of information security, expressed in Table 1. The first three attributes refer to information disregarding its form. The following attributes refer to providing data protection in ICT systems. Information is considered secured if all attributes of information security are provided.

Information security in public administration must be regarded in the context of realisation of missions of an institution and delivery of proper quality of the provided services, simultaneously providing attributes of information security. It is suggested to define information security in public administration as a state and a process in which (Szczepaniuk, 2016):

- Information security is achieved and sustained on a predetermined level of confidentiality, integrity, and accessibility;
- Security of provided services is achieved and sustained on a predetermined level of reliability, accessibility, and integrity of services;
- Authentication and accountability of entities, related to authentication of users utilising specific information and services are provided;
- Elements which constitute the public administration system are characterised with the ability to protect against current and future disruptions (threats) for functioning or loss of specific values – the system is resistant toward threats (internal, external, accidental, purposeful);
- Information and service users (employees in public administration) and information and service recipients (citizens, entrepreneurs, employees working in different public administration units) are aware of threats and are invulnerable to them;
- Perpetuators of security incidents (also internal offenders) have restricted possibilities to use cyberspace for purpose of generating threats by utilising vulnerabilities and gaps within the security system.

### 3.2. Information security threats in public administration institutions

Information security threats in public institutions can be analysed from the point of view of a whole country, a local authority unit, or a single institution. In the article, a single institution belonging to public administration system was focused on.

A public administration institution can be defined as a whole, separated from public administration system, established accord-

ing to legal rules, realising tasks (goals) in legally defined forms and utilising available resources. A public administration institution defined as above may be described using the following set of elements (Szczepaniuk, 2016):

$$U = \{L,\ I,\ M,\ F,\ C,\ O, R\} \tag{4}$$

key:

$U$ - public administration institution,
$L$ - human resources,
$I$ - information resources,
$M$ - material resources,
$F$ - financial resources,
$C$ - goals and norms (including the law),
$O$ - organisational, procedural and technical solutions,
$R$ - relations between elements of a public administration institution.

The main task of a public administration institution is realisation of public tasks related to decision making based on available information. Based on the system theory, decision making in an institution is realised based on processing input information into output information (see e.g. Chikere and Nwoka, 2015). Considering definition of an institution defined in (4) and the character of decision making in public administration, an institution is a set of cooperating elements which gather data (input data) and process them, emit and deliver feedback in order to achieve an adopted goal (output data). An example of the process described above is issuing an administrative decision based on documents delivered by parties of an administrative proceeding.

In a public administration institution, an executive subsystem and a management system may be differentiated. First of those realises processes related with realisation of public tasks. The other one realises management processes thus effecting required realisation of environment needs within the executive system. Functioning of a public administration institution may be realised using paper, electronic or mixed circulation of documents. It must be noted, that circulation of documents in an institution managed electronically is realised in a different way than in an institution with paper-based circulation of documents. Those models differ in, amongst others, the infrastructure utilised for circulation of documents, including also location and form of inflow (input data) and outflow (output data) of documents and the method of their processing and circulation. Electronic documents flow into an information system, not an executive system, as it is realised in case of a system with paper-based circulation of documents. Both in Poland, as well as over the world, many reports assessing level of advancement of e-administration (see e.g. e-Government Survey, 2018; The Global Information Technology Report, 2016) were developed. In practice, in most institutions in Poland, a mixed circulation of documents with use of IT systems (e.g. Electronic Platform of Public Administration Services – ePUAP), electronic public registers (e.g. National Registers System – SRP) and circulation of documents using office instructions (e.g. an official letter is delivered in a paper form to institution's department of administration) is in place.

A public administration institution characterised as above may be affected with various types of threats. It must be noted, that institutions with paper-based circulation of documents are at risk regarding other types of threats than institutions with electronic circulation of documents, whereas in a unit utilising simultaneously both solutions, both – information processed electronically and information processed traditionally may be at risk of security incident.

Relating the above considerations to the Clements general security model discussed in (3) and the definition of information security proposed in the article, information threats for information security in a public administration institution can be characterised. For this purpose, the following systemic situation is proposed for analysis (Sienkiewicz, 2013):

$$\Sigma = \langle S,\ O, R\rangle \tag{5}$$

key:

$\Sigma$- systemic situation,
$S$- system which is an object of information threats,
$O$- environment comprising of objects considered source of information threats
$R \subset S \times O$ – set of relations.

Then, the object of threats (system), which is a public administration institution, has a defensive potential: $P(s) \geq 0, s \in S$, whereas the source of threats is characterised with its destructive potential $P(o) \geq 0, s \in O$. On the $R$ set, a relation $Rz = Rz(o, s)$, was defined, which results in (Sienkiewicz, 2013):

$$\mathrm{V}_{o,s} o\ Rz\ s \Leftrightarrow P(o) \geq P(s) \tag{6}$$

That is – object $s \in S$ is threaten by $o \in O$.

Within source literature there are multiple classifications of information security threats (see e.g. Howard and Longstaff, 1998; Loch et al., 1992; Szczepaniuk, 2016). Security threatening situations in public administration institutions may occur in multiple dimensions, amongst others:

- Natural threats related to natural disasters, e.g. flood;
- Traditional information threats related to activities aimed at acquiring information, e.g. espionage;
- Threats originating in cyberspace covering attacks on information within ICT systems, e.g. man-in-the-middle attack (MITM)
- Threats resulting from reliability of IT systems, e.g. software errors (gaps);
- Purposeful actions by institution's employees, e.g. information theft;
- Threats occurring due to improper organisation and internal procedures of an institution, e.g. untrained employees generate a real threat; for instance, due to vulnerability toward social engineering attacks;
- Threats breaching civil rights e.g. breaching personal data, delivering information to unauthorised entities, identity theft.

Information security incidents in public administration institutions are conditioned on vulnerabilities which may occur in case of any of the indicated (4) elements of a public administration institution. It must be underlined, that every institution has its own specific characteristics, e.g. utilised IT hardware, dedicated IT systems, organisation of an IT system, which are characterised with specific vulnerability regarding information threats. Therefore, defence level of a public administration institution may be increased utilising information security management which should be determined by legal obligations, nature of operations realised by an institution and the need of continuous improvement.

### *3.3. The essence of information security management in public administration*

Information security management in public administration is an integral part of system management and it is related to rationalising the choice of measures which provide functioning of the system according to its purpose in a dangerous environment. Information security management undergoes the same principles as any other field of management – it has its goal, plans, policy, solutions regarding implementation, control and auditing instruments, accounting management and programs related to sustaining current results and continuous improvement and quality increase.

Takin into account considerations included in (4)–(6), the essence of information security management can be explained in

relations to the systemic situation described in (7)–(11), in which the following values are given (Sienkiewicz, 2015):

- external threats $A(t)$ resulting from the environment of a system, which correspond to the function of destructive threat potential,
- resistance of a system toward external threats $B(t)$, which corresponds to function of defensive potential (securing).

The above-indicated characteristics of a situation are random functions with known probability distributions:

$$F(a,t) = P\{A(t) < a\},$$
$$G(b,t) = P\{B(t) < b\},$$
$$t \in T \tag{7}$$

A generalised security factor of a system may be the probability, that threats will not exceed the acceptable (critical) level $a_o \geq 0$, while system resistance will be above the $b_o$ limit value, that is:

$$\beta(t) \equiv \beta(a_o, b_o) = P\{A(t) \leq a_o,\ B(t) > b_o\} \tag{8}$$

which leads to a system security assessment factor, provided statistical independence of the analysed values is delivered:

$$\beta(t) = F(a_o, t)[1 - G(b_o, t)] \tag{9}$$

Adopting the required system security level as $\beta_o > 0$, it can be indicated that in period $T$, the system is safe if in a given moment the following condition is realised:

$$\beta(t) \geq \beta_o, t_o < t \leq t_o + T \tag{10}$$

System security analysis often includes using simplified procedures which result in calculating probability:

$$P = p(P_s < P_o) \tag{11}$$

that is, the probability of occurrence of an event in which the general resistance (defensive potential) $P_s$ is higher than the general threat $P_o$ (Sienkiewicz, 2015).

Considering the above, the issue of information security management can be driven to optimisation of the distribution of security measures in relation to system penetration paths, in order to provide protection for the system. In other words, a $P_s$ level, which maximizes the security level $\beta$, can be defined. This generates a necessity to choose such security strategy out of the set of acceptable variants, for which the anticipated value of effects of a threat takes the minimal value, and the costs of implementation of a strategy will not exceed the accepted value. Therefore, implementation of protection must be preceded with defining limit values for results of threats and estimation of accepted value of financial assets which can be spent on security measures. This implies a necessity to adopt a specific methodology of information threat risk management, and choice of method for calculating costs.

In the practice of analysis of information threats, various risk assessment methods are used, e.g. OCTAVE - Operationally Critical Threat, Asset and Vulnerability Evaluation (see e.g. Alberts and Dorofee, 2003), CRAMM - CCTA Risk Analysis and Management Method (see e.g. Yazar, 2002), MEHARI - Method of Risk Analysis (see e.g. Mihailescu, 2012), FMEA - Failure Mode and Effect Analysis (see e.g. Schmittner et al., 2014), ISRAM – Information Security Risk Analysis Method (see e.g. Karaback and Sogukpinar, 2005). Moreover, risk management methods within norms, standards and good practice, e.g. ISO/IEC 27001 norm and the related norms (see e.g. ISO/IEC 27001; ISO 27005), COBIT methodology (see e.g. ISACA, 2013), NIST 800–37 (see e.g. NIST, 2018), have been developed.

As mentioned before, information security management requires an increase in specific costs, which in case of complex solutions may constitute a significant part of the budget of a given institution. In the source literature and in practical solutions, various methods for calculating costs in information security are applied, e.g. ROI method - Return on Investment, ROT method - Real Options Theory, UM method - Utility Maximization (see e.g. Schatz and Bashroush, 2017), ABC method - Activity-Based Costing, TDABC method - Time-Driven Activity-Based Costing (see e.g. Leszczyna, 2017), ALE method - Annual Loss Expectancy (see e.g. Sklavos and Souras, 2006; Tsiakis and Stephanides, 2005).

In summary, the issue of information security management in public administration can be expressed as (Sienkiewicz, 2013):

- minimising risk function, provided that the value of effects (usability) achieved due to operating of a system will not be below limit value (demanded), or
- maximising system efficiency function, provided that the risk function will not exceed accepted value.

This framework should be sustained with regard to the accepted limit values of effects of threats, and accepted costs dedicated for securing a system.

### 3.4. Implementation of information security management system

Realization of the theoretical framework related to providing information security in public administration relates to the necessity to implement Information Security Management System (ISMS). In the process of implementation of ISMS, various standards are applied, such as ISO/IEC 27001, BS 7799, ITIL and COBIT (see e.g. Susanto et al., 2011). In the article, the theoretical basis of implementation of ISMS is driven from the ISO/IEC 27001 norm, which is the recommended solution in Poland.

According to the ISO/IEC 27001 standard, an Information Security Management System is a „part of a holistic management system, based on the approach resulting from a business risk, which refers to establishing, implementing, utilization, monitoring, sustaining and improving information security. ISMS includes organizational structure, policies, planning actions, liabilities, practices, procedures, processes and resources" (Liderman, 2006).

The goal of an operating ISMS is to eliminate or minimize the risk of occurring information threats utilizing a set of planning, organizational, technical and control activities. ISMS is an element of organisation management system, which is characterised by organisational structure, security policy, realised processes and resources. Within the process of development of ISMS, the following stages, presented on Fig. 1. can be distinguished.

The essence of ISMS includes organizational and technical mechanisms in the aspect of providing information security, which should be adequate to the data interference risk. Analysis and risk assessment in information security constitutes the basis of implementation of ISMS in an organisation. The obligation to manage the risk for purpose of personal data protection and to provide cybersecurity is stated also within European Union documents - GDPR Regulation (O.J. EU L 119/1, 4.5.2016) and NIS Directive (O.J. EU L 191/1, 19.7.2016). Implementation of ISMS according to ISO/IEC 27001 and based on solutions indicated by the European Union and nationally, may be a complementary solution which includes a wide spectrum of legally protected information.

Risk management in information security requires stocktaking and assessment of resources which may be at risk. The resources are of specific value to an institution; therefore, the occurrence of a security incident generates specific consequences for an organisation. Fundamental for risk analysis is the identification of threats which are defined as „any phenomenon (process, event), unwanted from the point of view of an undisturbed operating of a system" (Sienkiewicz, 2013). The occurrence of a threat is facilitated by a so-called vulnerability, which is a weakness or a gap in the security

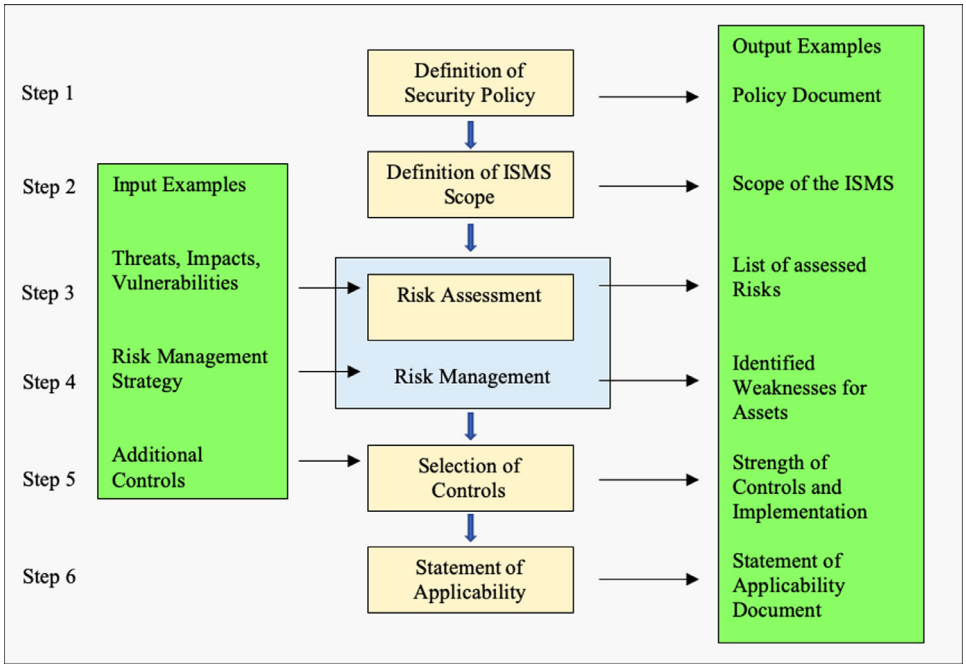


**Fig. 1. The ISMS Framework.**
*Source:* Based on ENISA, 2006

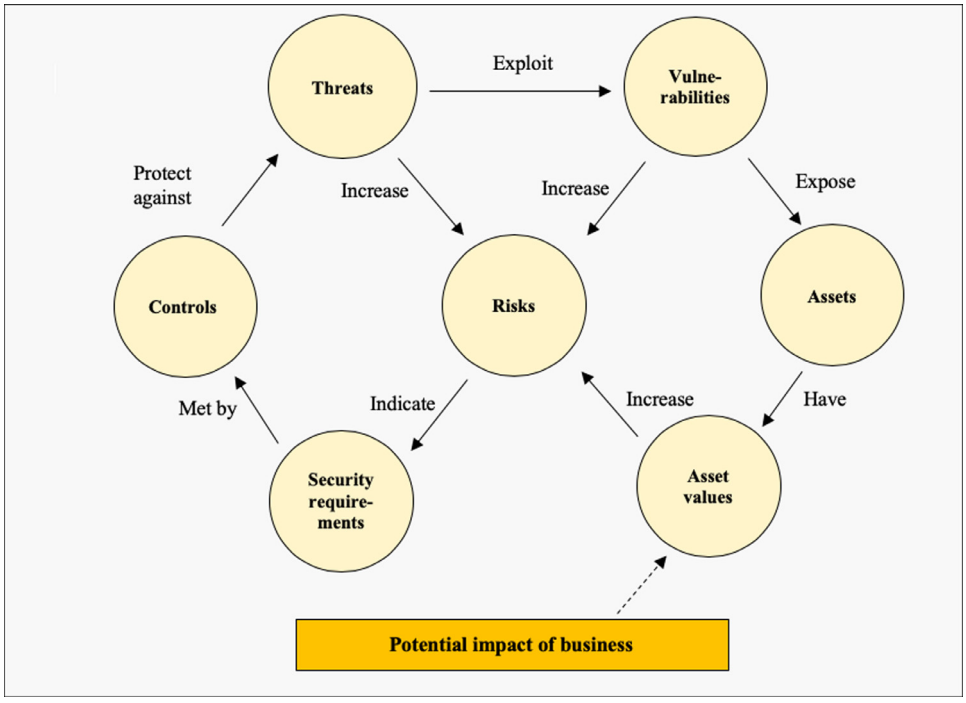


**Fig. 2. Diagram of interrelationships in risk management.**
*Source:* Based on Tupa and Steiner, 2006.

system of a given object. The relation between a threat and vulnerability, expressed with the probability of occurrence of a threat and the amount of loses generated by this threat, is referred to as the risk. Risk analysis indicates requirements in the aspect of security, which are implemented in the form of protection measures which minimize the risk. The characterised interrelationships in risk management are presented in Fig. 2.

The key element in the process of implementation of ISMS in a public institution is implementing proper protection measures. In the attachment A to the ISO/IEC 27001 norm, the following grouped list of protection measures is included amongst others: information security policy, organisation of information security, human resources security, assets management, access control, cryptography, physical and environmental security, operational security, communication security, obtaining, development and maintenance of a system, managing incidents of information security incidents, managing continuity of management and compliance (Brewer and Nash, 2010). These groups are detailed with recommended types of security measures and recommendations regarding implementation.

Security environment and internal conditions of an organisation are time variant; therefore, it is necessary to monitor and improve elements of ISMS. Within ISO/IEC norms regarding ISMS, within the whole structure of the processes, the Deming cycle (PDCA model), developed in the 1950s, was applied. This model illustrates a process of continuous upgrading of an institution and it is comprised of the following stages: plan, execute, verify, act. Regarding ISMS in public administration institutions, the PDCA model is a cycle of consecutive actions aiming to fulfil the main goal, which is achieving information security within an institution.

### 3.5. Research results

Theoretical analysis conducted in the article suggests the conclusion that efficient information security management should include complex management of the security of information resources, infrastructure dedicated for its processing, knowledge, and competence of workers, and security measures within the whole institution of public administration.

For the purpose of performing empirical research and presenting research results, it is assumed that the management process in the institution of public administration depends on the following factors:

- legal – defined by the regulations of common law, which enable the creation of conditions and rules of functioning of a public administration unit;
- procedural and organisational – covering a range of responsibility and internal regulations of a public administration unit;
- Physical and technical – covering physical and technical protection measures implemented in the institution of public administration;
- social (human factor) – related to the competence of employees of a unit;
- other resources of an organisation (e.g. capital), which influence the efficiency of the information security management system.

The adopted in the article research process model is characterised by the rejection of the postulate on the dominance of any of the organisational factors in the systemic concept of an organisation. Upgrading organisation is equivalent to the demanded shaping of the all analysed factors (see e.g. Sienkiewicz, 1989). Due to this fact, the empirical research has included legal, procedural, organisational, physical, technical, social and other elements and resources of an organization.

Empirical research was conducted using surveying with survey questionnaires. 50 public administration units took part in the research. In order to determine the influence of the European Union solutions (i.e. GDPR Regulation and NIS Directive) on information security management in the public administration in Poland, the research was performed in the years 2016 – 2019. Table 2 presents data regarding the number of chosen elements of a Security Management System in the researched entities in the years 2016 – 2019.

Results of the research in the field of organizational structure, procedures and internal documents in the years 2016 – 2017 have shown a little involvement of public administration units in the implementation of elements of ISMS. In the year 2016 – 18% of researched entities have applied organisational structure and in the year 2017 – 28%. None of the entities had implemented a certified ISMS compliant with ISO/IEC 27001. In the years 2016–2017, most entities have not developed documentation or procedures, or they were incomplete or outdated. amongst the identified irregularities, amongst others, the following were included: lack of information security policy, limited use of risk management, lack of vulnerabilities and information security incidents management. In the years 2018 – 2019, after implementing into Polish legal framework the European Regulation GDPR and the NIS directive, a significant increase in the number of entities with applied organizational structure and ISMS documentation has occurred. In the year 2018, 31 (62%) of the researched entities have implemented ISMS organizational structure, which indicates an increase in 34% regarding the previous year. In the year 2019, 84% of entities have established organizational structure. Research results indicate that also the number of entities with certified ISMS has increased – 7 in the year 2018, and 11 in the year 2019. In the years 2018 – 2019, a significant increase in the aspect of developing ISMS documentation and procedural solutions. The percentage of entities which in the year 2019 have developed ISMS documentation and procedures shaped as follows: information security policy (100%), risk management (76%), overviewing information security (74%), information security audit (74%), managing information security incidents (66%), vulnerabilities management (58%), continuity of operations management (58%) and external controls (18%). In the years 2016 – 2019 all of the researched entities were realizing stocktaking of hardware and software.

**Table 2**
Number of elements of ISMS in the researched institutions (years: 2016 – 2019).

| Researched elements | 2016 | 2017 | 2018 | 2019 |
|---|---|---|---|---|
| Organizational structure, procedures, internal documents | | | | |
| ISMS structural organization | 9 | 14 | 31 | 42 |
| Certified ISMS | 0 | 0 | 7 | 11 |
| Stocktaking of hardware and software | 50 | 50 | 50 | 50 |
| Information security policy | 18 | 21 | 43 | 50 |
| Risk management | 5 | 5 | 23 | 38 |
| Managing information security incidents | 1 | 3 | 28 | 33 |
| Managing vulnerabilities | 0 | 2 | 11 | 29 |
| Managing continuity of operations | 0 | 1 | 13 | 29 |
| Overviewing information security | 5 | 8 | 18 | 37 |
| Information security audit | 3 | 7 | 18 | 37 |
| External controls | 0 | 1 | 3 | 9 |
| Physical and technical security measures | | | | |
| Physical access control | 17 | 27 | 39 | 45 |
| IT systems access control | 3 | 9 | 29 | 42 |
| Monitoring use of IT systems | 0 | 2 | 11 | 27 |
| Backup copies | 1 | 5 | 18 | 32 |
| Anti-virus protection | 6 | 11 | 29 | 41 |
| Cryptographic security measures | 0 | 2 | 9 | 23 |
| Human factor | | | | |
| Improving skills within information security | 0 | 1 | 3 | 3 |
| Information security trainings | 2 | 2 | 12 | 17 |
| Personal data protection trainings | 25 | 25 | 42 | 50 |
| Defining range and responsibilities | 7 | 12 | 31 | 42 |
| Security of human resources | 2 | 7 | 27 | 38 |

*Source:* own work.

Another field indicated in Table 2. includes chosen physical and technical security measures. In the years 2016 – 2019, the physical access control mechanisms were the most often applied type of security measure in the researched entities. amongst used security measures, amongst others, the following were applied: monitoring, PIN code, and magnetic cards. In the years 2016 – 2017, most of the entities had not applied the mechanism of control of access to IT systems. Due to this, no measures which could prevent unauthorised access to information were applied, e.g. no requirement for password authentication, improper securing of access to a wireless network. In the following years, a significant increase in applying for protection against unauthorised access to IT systems has occurred. In the year 2016, none of the researched entities have monitored the use of IT systems. In the following year, this mechanism was applied only in two entities. In the following years, a significant increase in using IT systems monitoring has occurred – 11 entities in 2018 and 27 entities in 2019. Another researched field

**Table 3**
Research on influence of European Union solutions on ISMS in public administration.

| Variable A | Chi-2 test | | | C Pearson contingency coefficient | |
|---|---|---|---|---|---|
| | Empirical value Variable B: years 2016 - 2019 | Critical value | Hypothesis verification | Empirical value | Relation strength |
| Organizational structure, procedures, internal documents | 504,9 | 7,81 | positive | 0,69 | strong |
| Physical and technical security measures | 368,3 | | positive | 0,74 | strong |
| Human factor | 235,68 | | positive | 0,7 | strong |

*Source:* own work.

was the backup copies which in the years 2016–2017 in most of the researched entities were not developed or were developed and stored improperly. Research results, amongst others, indicated: lack of a sufficient number of applications realising backup copies and little knowledge about the necessity to create them. In the years 2018–2019, the number of entities in which backup copies were regularly created has increased. Cryptographic mechanisms were the most rarely used solution in the aspect of the researched field of security. Percentage of entities applying cryptographic protection shaped as follows: 0% (year 2016), 4% (year 2017), 18% (year 2018), 46% (year 2019).

Research results in the field of society have revealed that in the years 2016 – 2019, in most of the researched entities, employees were not increasing their skills, e.g. through external courses, training or post-graduate studies. According to directors of these entities, insufficient funds were the reason for this situation. In the years 2016 – 2019, only in two entities, training in information security, including threats, results and consequences and protection providing measures, were organized. In the following years, an increase in the number of realized pieces of training occurred: 12 in 2018 and 17 in 2019. Significantly more often, personal data protection trainings were provided, which in the years 2016–2017 were conducted in half of the researched entities. After applying the GDPR Regulation in Poland, which regulates personal data protection, trainings were performed in most entities, i.e. 84% (the year 2018) and 100% (the year 2019). In the years 2016–2017, defining range and responsibility for the purpose of ISMS occurred in a limited manner. In the following years, most entities have established range and competence in the aspect of information security management. In the years 2016–2017, in most entities, no security of human resources was delivered. These irregularities were related to excessive granting of permissions in IT systems, i.e. authorities beyond the range of duties. Moreover, a problem of not denying or too late denying of authority in IT systems was identified. amongst the reasons of the occurred irregularities, too small number of employed IT specialists or work overload, were indicated. In the years 2018–2019, irregularities related to security of human resources were nullified significantly in most of the researched entities.

Analysis of the results enables to suspect, that there is a relation between information security management in public administration and implementation of European Union solutions – GDPR Regulation and NIS Directive, in the year 2018 into Polish legal order. This hypothesis has been verified using a Chi-2 relation test and the C Pearson contingency coefficient (Table 3).

Statistical analysis of relations between elements: variable A (organisational structure, procedures, internal documents, physical and technical security measures, human factor) and variable B (year of research), provides confirmation of the formulated hypothesis. There is a relation between the implementation of elements of ISMS in public administration and the years of research. Since the year 2018, public administration entities in Poland are obliged to comply with the regulations contained in GDPR Regulation and NIS Directive, which implicates positive changes in the process of information security management in public administration.

In the year 2019, employees of public administration were also researched in the aspect of knowledge on threats, effects of security incidents, security measures, regulations of common law and ISMS documentation. The survey's questionnaire was completed by 10 persons from each researched entity (500 respondents overall). For the purpose of analysis of research results, a hypothesis on the existence of relations between knowledge and awareness of respondents and education (IT, not IT) and realised training, was adopted. amongst the respondents, 74 persons had a university degree in IT, while 170 persons were assigned for training. Table 4 shows knowledge of the respondents within fields defined by the variable A, divided according to obtained education and performed training (variable B). Relations between variables was researched using Chi-2 test and the C Pearson contingency coefficient (Table 5).

Statistical analysis of relations between the researched variables has shown that there is a strong relation between obtained education and knowledge on threats and security measures. Research results indicated that there is a relation between education and

**Table 4**
Knowledge of the respondents in the researched entities.

| Variable A | Variable B: education | | | | Variable B: training | | | |
|---|---|---|---|---|---|---|---|---|
| | IT | | other | | realized | | Not realized | |
| | Has knowledge | Has no knowledge | Has knowledge | Has no knowledge | Has knowledge | Has no knowledge | Has knowledge | Has no knowledge |
| Threats | 74 | 0 | 62 | 364 | 129 | 41 | 7 | 323 |
| Effects | 70 | 4 | 76 | 350 | 132 | 38 | 14 | 316 |
| Security measures | 73 | 1 | 51 | 375 | 117 | 53 | 7 | 323 |
| Legal regulations | 32 | 42 | 210 | 216 | 145 | 25 | 97 | 233 |
| ISMS documentation | 61 | 13 | 211 | 215 | 160 | 10 | 112 | 218 |

*Source:* own work.

**Table 5**
Research on influence of education and training on knowledge of the respondents.

| Variable A | Chi-2 test | | | C Pearson contingency coefficient | |
|---|---|---|---|---|---|
| | Empirical value Variable B: education | Critical value | Hypothesis verification | Empirical value | Relation strength |
| Threats | 288,1 | 3,84 | positive | 0,61 | strong |
| Effects | 235,1 | | positive | 0,57 | moderate |
| Security measures | 316,5 | | positive | 0,62 | strong |
| Legal regulations | 1,4 | | negative | – | – |
| ISMS documentation | 31,2 | | positive | 0,24 | weak |
| Variable A | Variable B: training | | | | |
| Threats | 348,1 | 3,84 | positive | 0,64 | strong |
| Effects | 328,4 | | positive | 0,62 | strong |
| Security measures | 326,7 | | positive | 0,63 | strong |
| Legal regulations | 140,8 | | positive | 0,47 | moderate |
| ISMS documentation | 166,4 | | positive | 0,5 | moderate |

*Source:* own work.

knowledge, i.e. moderate in the aspect of effects and weak in the field of ISMS documentation. No relation between IT higher education and knowledge of regulations of common law was indicated.

In summary, research results have shown irregularities in implementation of ISMS in public administration in Poland, in the years 2016–2017. Implementation of European Union solutions in Poland, in the aspect of personal data protection and cybersecurity, have implicated positive changes in the aspect of organising ISMS in public administration entities. A need to broaden knowledge and to raise the awareness of employees of public offices, in the aspect of information security management, was indicated.

## 4. Conclusions and recommendations

Growth tendencies of information threats and changes in the legal system impose on public administration entities an obligation to introduce, implement and improve Information Security Management System. With regard to the object and the aim of the research, the following conclusions were formulated:

- Providing information security requires a systemic approach and it should be one of the elements of operations of public administration entities. Information security in public administration should be perceived in the context of realising missions of the institutions and delivering sufficient quality of provided services, simultaneously providing attributes of information security.
- A public administration institution is an organisational structure separated from public administration system, which realises public tasks. Occurrence of an information security incident may decrease the level of delivered services, or it may cause lack of availability of services. Situations of threats regarding information security in public administration institutions may consider its various elements and resources. Individual units have their characteristic features, e.g. utilised IT hardware, dedicated IT systems, organisation of an IT system, which are characterised with specific vulnerability regarding information threats. Defence level of public administration institutions should be increased utilising information security management.
- The efficiency of information security management in public administration is determined by its resistance toward the occurrence of dangerous situations (information security incidents). The issue of information security management can be broken down to optimisation of the distribution of security measures in relation to probable threats, in order to provide security for an entity. This determination should be realised considering the accepted limit values for the effects of threats and the accepted costs dedicated to security.
- ISMS includes planning, procedural, organisational, physical, technical and social solutions, which include information threat risk management and responsibilities defined in regulations of law.
- ISMS includes planning, procedural, organisational, physical, technical and social solutions which should be adequate to the risk of interference in data and responsibilities defined in regulations of law. Implementation of ISMS requires establishing, implementing, utilising, monitoring and improving all elements of the system.
- Empirical research in the aspect of the implementation of ISMS has shown, that in the practice of operating of administrative entities, approaches to the protection of information are various. In the years 2016–2017, in most entities, no basic elements of ISMS were implemented, or provisional attempts to implement a security system were undertaken, e.g. actions of individual departments which were not coordinated within the whole institution. Problematic fields and irregularities were identified, which include amongst others: lack of organising an ISMS, incomplete or outdated ISMS documentation, lack of regular risk assessment, lack of overviews, audits or controls, limited use of physical and technical security measures, no training or professional development. European Union solutions, i.e. GDPR Regulation and NIS Directive, have influenced an increase in the level of information security in public administration in Poland and significantly reduced the occurrence of identified irregularities.
- Empirical research in the aspect of knowledge and awareness of employees of public offices have indicated a lack of common knowledge on information security management. Moreover, a relation between the level of knowledge of the respondents and IT education and realised training, was indicated. It is proposed to increase the number of employed IT specialists and information security specialists and conducting obligatory training covering all employees in public administration. Training should provide delivery of knowledge, control of knowledge and identification of employees requiring additional training.

The results of theoretical and empirical research may be useful in implementation of ISMS in public administration institutions and in continuation of the research regarding information security. The authors recommend the theoretical deliberations contained in the article to be taken into account while designing and implementing ISMS. Effectiveness of mechanisms for protection against information security in public units depends a systemic approach which includes managing all elements of a public adminis-

tration institution. Realisation of the above provisions should be performed considering specific nature and missions of individual public institutions. Identification of information threats and risk management constitute significant elements of ISMS. These processes facilitate system improvement and they generate a possibility to eliminate vulnerabilities and selection of proper security measures. This enables to reach proper defensive potential of a system, adequate regarding destructive potential of a threat, which are characterised in (4)–(11). However, it must be underlined, that public administration units operate within a volatile security environment, thus security level is not considered a permanent state and it requires constant monitoring and improvement.

Empirical research results presented in Tables 2–5 have shown, that there is a statistical relation between information security management in a public institutions and implementation into Polish legal order, in 2018, European Union solutions, i.e. the GDPR regulation and the NIS Directive. The Authors recommend the indicated results of empirical research to be utilised in work of system analysts and planners in the process of designing and implementation of ISMS in public administration institutions. It is advised, that the elements of ISMS presented in Table 2 were regarded obligatory elements of an organisation structure and procedural solutions of public administration institutions. These elements constitute an attempt to standardise solutions used in public administration institutions and they represent possibilities brought about by systemic management of information security. Empirical data indicate practical aspects of designing and maintaining ISMS, which should be further developed in form of analysis of detailed procedures and models regarding, amongst others:

- methods of assessing threat vulnerability of institutions,
- methods of performing risk management of information threats,
- methods of training employees of public administration institutions,
- methods of selecting security measures,
- ISMS auditing methods,
- methods of integrating a public services quality management system with an information security management system,
- programs including practical hints for public administration units for purposes of ISMS implementation
- directions of cooperation, exchange of experience and good practices between institutions.

In order to realise the above provisions, it is reasonable to increase financial outlays for implementation of ISMS in public administration units. Moreover, there is a deficit of information security specialist on the market. The basic task of higher education facilities is development of programs and specialisations orientated toward educating future information security experts. The authors recommend the elements contained in Table 2 to be reflected in learning plans within programs educating future employees of public administration.

The issue of information security management in public administration institutions requires further research. This need is justified by the fact, that security is not considered a permanent state. Moreover, both in Poland as well as over the world, there are problematic fields in designing and implementation of ISMS. Analysis of global security environment of public administration institutions enables to assume, that threats will evolve and more advanced methods of conducting cyberattacks will develop. Public administration will be also a participant of further development of digitalisation, which will probably render another transformation of local governments. It can be assumed, that this will lead to changes on multiple levels, amongst others: legal, organisational, technological. These issues cover a wide spectrum of inter-disciplinary in nature problems; therefore, the authors recommend conducting research supported by cooperation of Polish and foreign scientific facilities, higher education facilities and companies. Due to the above, in further research, it is recommended to discuss the need of constant international collaboration within scope of information security management in public administration institutions.

## Declaration of Competing Interests

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

## References


Alberts, Ch., Dorofee, A., 2003. Managing Information Security Risks. The OCTAVE Approach.. Addison-Wesley. USA, Boston.

Alhassan, M.M., Adjei-Quaye, A., 2017. Information security in an organization. Int. J. Comput. Volume 24 (No. 1), 100–116. https://www.researchgate.net/publication/314086143_Information_Security_in_an_Organization. Accessed 11 April 2019.

Barczak, A., Sydoruk, T., 2003. Bezpieczeństwo systemów informatycznych zarządzania. Warsaw: Bellona. Poland.

Brewer, D., Nash, M. (2010). Insights into the iso/iec 27001 annex a, http://www.gammassl.co.uk/research/27001annexAinsights.pdf. Accessed 27 March 2019.

Brooks, D.J., 2009. What is security: definition through knowledge categorization. Secur. J. 23 (3), 225–239. doi:10.1057/sj.2008.18.

Chikere, C.C., Nwoka, J., 2015. The systems theory of management in modern day organizations - A Study of aldgate congress resort limited port harcourt. Int. J. Scientif. Res. Publ. Vol. 5 (Iss. 9), 1–7. https://pdfs.semanticscholar.org/d1e4/03a4a017d00b081122c2a0abd1d7317f14fe.pdf. Accessed 20 October 2019.

Degaut, M., 2015. What is security? Revista Brasileira de Inteligência 9–28. https://www.researchgate.net/publication/310495076_What_is_Security. Accessed 09 April 2019.

Dz.U. [Journal of Laws] of 2012, item 526. (2012) Rozporządzenie rady ministrów z dnia 12 kwietnia 2012 r. w sprawie krajowych ram interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych. Poland.

Dz.U. [Journal of Laws] of 2018, item 1000. (2018) Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych. Poland.

Dz.U. [Journal of Laws] of 2018, item 1560. (2018) Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Poland.

e-Government Survey (2018). Department of economic and social affairs. United Nations. New York 2018. https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2018-Survey/E-Government%20Survey%202018_FINAL%20for%20web.pdf. Accessed 15 October 2019.

ENISA, (2006). Risk Management: Implementation principles and Inventories for Risk Management/Risk Assessment methods and tools: Survey of existing Risk Management and Risk Assessments Methods. Technical Department of ENISA Section Risk Management. https://www.enisa.europa.eu/publications/risk-management-principles-and-inventories-for-risk-management-risk-assessment-methods-and-tools. Accessed 16 November 2019.

ENISA. (2017). Priorities for eu research analysis of the ecso strategic research and innovation agenda (SRIA). https://www.enisa.europa.eu/publications/priorities-for-eu-research. Accessed 14 March 2019.

Hoffman, L.J., 1982. Poufność w Systemach Informacyjnych. WNT. Poland, Warsaw.

Howard, J.D. & Longstaff, T.A. (1998). A common language for computer security incidents. https://www.osti.gov/servlets/purl/751004. Accessed 20 October 2019.

ISACA. (2013). COBIT 5 for risk. https://m.isaca.org/COBIT/Documents/COBIT-5-for-Risk-Preview_res_eng_0913.pdf. Accessed 14 April 2019.

ISO/IEC 27001: 2013, Information technology – Security techniques – Information security management systems - Requirements.

ISO/IEC 27005: 2018, Information technology – Security techniques – Information security risk management.

Janczewski, L.J., Cealli, W. (Eds.) (2015). Cyber conflicts and small states, New Zealand 2015.

Karaback, B., Sogukpinar, I., 2005. ISRAM: information security risk analysis method. Comput. Secur. 24 (2), 147–159. https://www.sciencedirect.com/science/article/pii/S0167404804001890. Accessed 14 April 2019.

Leszczyna, R., 2017. Metoda szacowania kosztu zarządzania bezpieczeństwem informacji i jej przykład zastosowania w zakładzie opieki zdrowotnej Nr 46 (2017), pp. 319-330. Warsaw. Poland.

Liderman, K., 2006. Zarządzanie ryzykiem jako element zapewnienia odpowiedniego poziomu bezpieczeństwa teleinformatycznego Nr 23/2006, pp. 44, Warsaw. Poland.

Liderman, K., 2012. Bezpieczeństwo Informacyjne. PWN. Poland, Warsaw.

Loch, K.D., Carr, H.H., Warkentin, M., 1992. Threats to information systems: today's reality, yesterday's understanding. MIS Q. Vol. 16 (No. 2), 173–186. https://www.researchgate.net/publication/220259924_Threats_to_Information_Systems_Today's_Reality_Yesterday's_Understanding. Accessed 20 October 2019.

Mihailescu, V.L., 2012. Risk analysis and risk management using mehari. J. Appl. Bus. Inf. Syst. 3 (4), 143–161. 2012 https://pdfs.semanticscholar.org/0d21/f50d42a2699b4ab5174edf4968b128b7d6b3.pdf. Accessed 11 April 2019.

Możdżeń-Marcinkowski, M., 2012. Introduction to Polish Administrative Law. C.H. Beck. Poland, Warsaw.
NIK, 2016. Zapewnienie Bezpieczeństwa Działania Systemów Informatycznych Wykorzystywanych Do Realizacji Zadań publicznych. Informacja o wynikach Kontroli. NIK. Poland, Warsaw https://www.nik.gov.pl/kontrole/P/15/042/KPB/.
NIST. (2018). Risk management framework for information systems and organizations. Accessed 14 April 2019. doi:10.6028/NIST.SP.800-37r2.
O.J.EU L 119/1, 4.5.2016. (2016) Regulation (UE) 2016/679 of the European Parliament and of the council of 27 april 2016 on the protection of natural persons with regard to the processing of the personal data and on the free movement of such data, and repealing directive 95/46/EC (General data protection regulation).
O.J. EU L 191/1, 19.7.2016. (2016) Directive (EU) 2016/1148 of the European Parliament and of the council of 6. july 2016 concerning measures for a high common level of security of network and information systems across the union.
Schatz, D., Bashroush, R., 2017. Economic valuation for information security investment: a systematic literature review. Inf. Syst. Front. Vol. 19 (Iss. 5), 1205–1228. https://link.springer.com/article/10.1007%2Fs10796-016-9648-8. Accessed 17 April 2019.
Schmittner, Ch., Gruber, T., Puschner, P.P. & Schoitsch, E. (2014). Security application of failure mode and effect analysis (FMEA) in computer safety, reliability, and security: 33rd international conference. pp. 310–325. Florence. Italy. https://www.researchgate.net/publication/290751391_Security_Application_of_Failure_Mode_and_Effect_Analysis_FMEA. Accessed 11 April 2019.
Sienkiewicz, P., 1989. Systemy Kierowania. Wiedza Powszechna. Poland, Warsaw.
Sienkiewicz, P., 1995. Analiza Systemowa. Bellona. Poland, Warsaw.
Sienkiewicz, P., 2010. Systems analysis of security management. Scientif. J. Maritime Univ. Szczecin 24 (96), 93–99 2010.
Sienkiewicz, P., 2013. 25 Wykładów. AON. Poland, Warsaw.
Sienkiewicz, P., 2015. Podstawy inżynierii systemów bezpieczeństwa. In: Sienkiewicz, P. (Ed.), Inżynieria Systemów Bezpieczeństwa. PWE. Poland, Warsaw, pp. 4–18.
Sklavos, N., Souras, P., 2006. Economic models and approaches in information security for computer networks. Int. J. Netw. Secur. Vol. 2 (No. 1), 14–20. https://pdfs.semanticscholar.org/16ef/df667e5aee3270d5c2d7987c05dcd15876c2.pdf. Accessed 18 April 2019.
Stańczyk, J., 1996. Współczesne Pojmowanie Bezpieczeństwa. PAN. Poland, Warsaw.
Stokłosa, J., Bilski, T., Pankowski, T., 2010. Bezpieczeństwo Danych w Systemach Informatycznych. PWN. Poland, Poznan.
Susanto, H., Almunawar, M.N., Tuan, Y., 2011. Information security management system standards: a comparative study of the big five. Int. J. Electr. Comput. Sci. IJECS-IJENS Vol: 11. No: 05, 2011 https://www.researchgate.net/publication/228444915_Information_Security_Management_System_Standards_A_Comparative_Study_of_the_Big_Five. Accessed 20 April 2019.
Szczepaniuk, E.K., 2016. Bezpieczeństwo Struktur Administracyjnych w Warunkach Zagrożeń Cyberprzestrzeni Państwa. AON. Poland, Warsaw.
Tsiakis, T., Stephanides, G., 2005. The economic approach of information security. Comput. Secur. 24 (2), 105–108. 2005 https://www.sciencedirect.com/science/article/pii/S0167404805000209?via%3Dihub. Accessed 19 April 2019.
Tupa, J., Steiner, F., 2006. Implementation of information security management system in the small healthcare organization. J. Telecommun. Inf. Technol. 52–58. https://www.il-pib.pl/czasopisma/JTIT/2006/2/52.pdf. Accessed 21 April 2019.
Vogt, W.P., Johnson, R.B., 2015. The SAGE Dictionary of Statistics & Methodology. A Nontechnical Guide for the Social Sciences. SAGE Publications, USA.
Yazar, Z., 2002. A qualitative risk analysis and management tool – CRAMM. SANS Institute. https://pdfs.semanticscholar.org/3743/6a533bcbcd1bb42000383eae445840e5cefc.pdf. Accessed 11 April 2019.
The Global Information Technology Report. (2016). Growth and jobs in a hyperconnected world. word economic forum and INSEAD. Geneva. http://www.cdi.org.pe/InformeGlobaldeInformacion/doc/WEF_GITR_Full_Report.pdf. Accessed 20 October 2019.
WEF (2019). The global risks report 2019. 14th edition. world economic forum. Geneva. http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf. Accessed 13 March 2019.
Zibran, M.F. (2007). CHI-Squared test of independence. https://pdfs.semanticscholar.org/0822/f125a21cfbd05e5e980c8017499fb966568f.pdf. Accessed 05 April 2019.

**Dr inż. Edyta Karolina Szczepaniuk:** Doctor of Social Science in the field of security sciences. Graduate with majors in the fields: administration, national security and computer science. She is an academic at the Polish Air Force University (Poland). Within the scope of her scientific interests, amongst others, there are: information security, cybersecurity, e-administration, Management Information Systems, databases and systems programming. Author of numerous publications within this scope.

**Dr Hubert Szczepaniuk:** Graduate of doctoral studies in the field of computer science in technical science at the Faculty of Cybernetics of the Military University of Technology in Warsaw. In the year 2015 he has defended a Ph.D.dissertation. He is an academic employee at the Warsaw University of Life Sciences WULS-SGGW in Warsaw. Research interests apply to computer science, management and quality sciences, cybersecurity. Author of numerous publications within this scope. His activity also includes programming in Python, Java and C#.

**Professor dr hab. Bogdan Klepacki:** Head of the Department of Logistics at the Warsaw University of Life Sciences, former Vice-Rector of Warsaw University of Life Sciences. Doctor honoris causa of the University of Agriculture in Krakow. Author of 570 articles and books on economics, management and logistics, adaptation of enterprises to changing economic conditions. Promoter in 27 doctoral courses. He cooperated with universities from several countries, an active participant of several dozen foreign, as well as Visiting professor. He managed 2 international and 9 national research topics. Member of the Committee of Economic Sciences of the Polish Academy of Sciences.

**Dr hab. inż. Tomasz Rokicki:** In 2006 he obtained academic degree of Ph.D. of economic sciences in terms of economy awarded by a resolution of the Agricultural Economics Department Board in the Warsaw University of Life Sciences (WULS – SGGW). Since 2007 have been working as an Assistant Professor at the Faculty of Economic Sciences in the WULS. On February 27, 2018, he obtained a post-doctoral degree – habilitation. His-academic achievements contains 10 monographs, over 120 articles in scientific journals and collective monographs. Research interests apply to economy, (micro and macro economy), economic geography, logistics (above all transport problems), management of information.