ZESZYTY NAUKOWE AKADEMII MARYNARKI WOJENNEJ
SCIENTIFIC JOURNAL OF POLISH NAVAL ACADEMY

2016 (LVII) 4 (207)

DOI: 10.5604/0860889X.1229758

Tomasz Sobczyński*

THE PRINCIPLES OF CLASSIFIED INFORMATION PROTECTION HANDLED IN COMMUNICATION AND INFORMATION SYSTEMS WITHIN THE REALISATION OF EUROPEAN DEFENCE AGENCY RESEARCH PROJECTS

ABSTRACT

The article presents the aspects of Communication and Information Systems security principles for classified Information Security Management System implemented within the realization of European Defence Agency research and technology projects. In the content of article, author characterised the rules and procedures, resulting from the legal acts, which regulates IT security procedures of classified information processing, obtained during the realisation of research process. Special attention has been focused on the European Defence Agency projects during which common IT security procedures are very important to provide not only the proper level of secrecy but also to ensure confidentiality, integrity and availability of all information processed during the research process.

Key words:
classified information, sensitive information, IT security, facility security, risk assessment, dissemination of EUCI, risk level valuation, accreditation and certification process.

INTRODUCTION

Contemporary world, addicted to technology, has completely changed the way of information processing. The development of IT sector caused that creators of Information Security Management Systems (ISMS) have to consider new aspects of risk

* Polish Naval Academy, Faculty of Navigation and Naval Weapons, Śmidowicza 69 Str., 81-127 Gdynia, Poland; e-mail: t.sobczynski@amw.gdynia.pl

management, confidentiality assurance or physical security features that occurs simultaneously with new information processing methods. All institutions and organizations connected to public or private sector are increasingly reliant on automated and interconnected IT systems to perform their essential functions. The benefits of such activities include improved information processing and communication. However, the factors that speed of processing and access to information, also increase the risks of computer intrusion, fraud, and disruption. Information systems are in danger not only of risk from malicious actions or accidental user errors but also from natural and man-made disasters. In recent years, systems have become more susceptible to these threats because computers have become more interconnected and, thus, more interdependent and accessible to a larger number of individuals. In addition, the number of individuals with computer skills is increasing, and intrusion, or 'hacking', techniques are becoming more widely known via the Internet and other media.

Information Assurance (IA) in the field of communication and information systems used during realisation of research European Defence Agency (EDA) projects is the confidence that such systems will protect the information they handle and will function as they need to, when they need to, under the control of legitimate users. Effective IA, implemented by all participants of the project, shall ensure appropriate levels of confidentiality, integrity, availability, non-repudiation and authenticity for all information processed during the research procedure. IA shall be based on a risk management process which is fulfilled by all participants of the research projects, and what is more, organised and implemented on principles, which are based on legal acts regulating area of information security in EU.

This article, focused on procedures and principles, connected with organisation of IT security systems, which are in fact crucial element for all institutions attempting to be awarded with execution of EDA defence and security research projects marked with appropriate confidentiality level.

INFORMATION ASSURANCE PRINCIPLES

Information Security, which is more accurately called Information Assurance, is now set up in three major concepts, also understood as an attributes, determining desirable level of security — those of *Confidentiality, Integrity* and *Availability (CIA)* [7, 13]. Managing these attributes is critical and since information has increasingly become one of the modern currencies of society, the preservation of assurance in

an appropriate and cost effective manner has become one of the most important elements in the supervision policies of all institutions, organizations or companies in all sectors, of all sizes and in all locations. CIA attributes are especially important considering the proper information management process within the realization of research projects in aspect of sensitive data exchange and handling procedure.

'Confidentiality is understood as the property that information is not made available or disclosed to unauthorised individuals, entities or processes' [6].

Information especially with classification level has to be applicable only to limited number of individuals because of its nature, its content or because its wider distribution will result Information Security Management Principles in undesired effects including legal or financial penalties and loss of respect. Restricting access to information to those who are granted with specific security clearance of an appropriate type and classification level in order to meet the legal requirements and also have a 'need to know', is good practice and is based on the principle of confidentiality. Organising control system to ensure confidentiality form a major part of the wider aspects of Information Assurance management like personnel security or physical security mechanism. Another basic principle of Information Assurance is maintaining of information integrity, what is understood as 'the property of safeguarding the accuracy and completeness of assets' [6]. Information is only useful if it is complete and accurate, and remains so. These aspects is often critical and ensuring that only certain people have the appropriate authority to modify or delete information. Planning IT system, the organizers have to consider 'the property of information to be accessible and usable upon demand by an authorised entity' [6], what means availability of information. If information is not available on demand, is not information at all but irrelevant data. In an ideal world, all important information can be locked up in a very secure safe and never allowed to be accessed, it is just about perfect assurance but naturally totally impractical. With development of technology, difficulties with ensuring availability have increased very significantly, nowadays the IT systems aim to remain available at all times, preventing service disruptions due to power outages, hardware failures, and system upgrades. Therefore, there will always be a compromise between security in its purest sense and the availability of the information [5].

This compromise has to be acknowledged throughout all aspects of Information Assurance designed for EDA classified research project's needs, and what is more a proper solutions to reduce threats and vulnerabilities of IT systems simultaneously with responding countermeasures has to be implemented thru all IT system lifecycle [3, 14].

THE LIFECYCLE IN IT SECURITY

To fill the IA objectives and achieve the aspired level of information security during the research process, the designers of ISMS have to understand how IT risks can threaten the fulfilment of tasks and research processes in context of the confidentiality, integrity, and availability of information. Being based on ISMS principles, the IT system live cycle contain of five stages: planning, projecting, initiation, exploitation and withdrawal. The very main and unconditional principle of IA during entire live cycle, is to reduce the risk of appearance of incidents connected with loss or unauthorised access to classified information processed in IT system. The role and interaction of each individual involved in the realisation of the research project with regard to its security shall be identified for each stage of the classified IT system life-cycle [5, 10].

Therefore, during the initiation stage, organizers of the system have to establish needs in the range of the processing of secret information in the IT system, and defines in the peculiarity[7]:

1. Destination of the IT system and what the system will serve for.
2. Maximum level of information classification to be processed in the IT system.
3. Type of safety work mode of the IT system.

There are three safety work modes generally accepted for the classified IT systems use purposes, which are categorized through the organization procedure of personal access to the system:

- dedicated work mode:
  - all users are authorized to access information of the highest classification level processed in this IT system,
  - and all users have the justifiable need of the access to all classified information processed in the IT system;
- comprehensive mode work:
  - all users are authorized to access information of the highest classification level processed in this IT system,
  - but not all users have the justifiable need of the access to all classified information processed in the IT system;
- multi-level (or mixed) work mode:
  - not all users are authorized to access information of the highest classification level processed in this IT system,

- and not all users have the justifiable need of the access to all classified information processed in the IT system.

4. Number of IT system users.
5. Localization of IT system.

When the IT system organizers have gathered all the information resulting from the initiation stage, the projecting stage can be proceed then. During this stage the preliminary risk assessment and safety measures selection has to be done. Moreover, the accreditation plan of the IT system has to be coordinated and accepted with accreditation entity. National Security Authority (NSA) of each EU State Member, responsible and authorised by multinational agreements to operate in the IT security of information area, have to provide the schedule and requirements to obtained accreditation process [1, 2]. All aspects of IT system, including its technical and non-technical security measures, shall be subject to security testing during the accreditation process to ensure that the appropriate level of assurance is obtained and to verify that they are correctly implemented, integrated and configured. Additionally, at this stage, a settlements to recognise cryptographic and TEMPEST[1] assurance take place and also safety requirements documentation of IT System have to be done.

After the accreditation and certification process, when the classified IT system has passed all safety examination with positive outcome and has been granted with a proper certificate, the exploitation stage can begin.

Throughout this stage a compliance of IT system with safety exploitation documentation has to be preserved and what is more continuity of a risk management process has to be also assured. To verify the correctness of applied safety measures and IT system work procedures, the personnel in control of risk management and safety procedures are in charge of periodically safety tests execution. If some weaknesses of the ISMS occurred and there is a need to implement some changes or modification to improve the level of security connected with safety measures, the changes are possible to implement after safety documentation upgrade in the form of annexes and positive opinion expressed by accreditation authority [9].

The last stage of IT system live cycle is withdrawal stage, when organizers of the IT system have decided that particular system is going to be turned off the exploitation. The significant moment during the EDA research and technology

[1] 'TEMPEST' means the investigation and control of compromising electromagnetic emanations and the measures to suppress them. Definition according the decisions *Council Decision of 31 March 2011 on the security rules for protecting EU classified information (2011/292/EU)*, p. 59.

projects is strictly connected with the last stage of the project when all classified materials has to be transferred to the leader of the project. In this moment individual contributors of the project can make the decision about withdrawal of the classified IT system. Procedure of withdrawal impose the obligation of official declaration about starting the IT system turn off process. The declaration has to be send to accreditation authorities altogether with certificate granted to the IT system during the accreditation process. The most important part of the withdrawal stage is connected with further proceedings of classified information stored in memory resources of the IT system. Basically all classified assets can be transferred to the other certified It system, or simply deleted. Considering the risk of uncontrolled lost or unauthorized access to the deleting files, this procedures has to be realised according to the strict rules defined in safety exploitation documentation. Detailed procedures have to be implemented according the proceedings with electronic devices and memo resources, especially when these equipment is planned to reuse [1, 2, 15].

This stage is final stage of classified IT system live cycle. Ensuring security shall be a requirement throughout the entire life-cycle from initiation to withdrawal from service. Only strictly proceedings according to the IA rules, designed, deployed and monitored by research and technology project ISMS creator, let the classified assets remain secure from the danger of unauthorised access. The role and interaction of each actor involved in IA with regard to its security shall be identified for each phase of the life-cycle. To be sure that our IA is confident and ISMS is functioning properly, the risk assessment and management process has to be performed with very high attention and awareness of the threats that can have the direct or indirect impact on the designed classified IT system. What is more, security assessments, inspections and reviews shall be performed periodically during the operation and maintenance of an IT system and when exceptional circumstances arise [8].

RISK ASSESSMENT AND MANAGEMENT

The idea of the ISMS assumes the adequacy of security measures implemented to reduce the risk in reference to identified levels of risk [9]. The risk management process is essential to achieved the anticipated effect of designing ISMS for specific area of classified research projects [1]. Security risk management shall be an integral part of defining, developing, operating and maintaining classified IT system.

Risk management (assessment, treatment, acceptance and communication) shall be conducted as an iterative process jointly by representatives of the system owners, project authorities, operating authorities and security approval authorities, using a proven, transparent and fully understandable risk assessment process [5].

Risk assessment is the first process in the risk management methodology. The organizers of IT systems planned to be used within the project realisation, are obliged to use risk assessment to determine the extent of the potential threat and the risk associated with an IT system throughout all live cycle of the project [11].

Risk is a function of the probability of a given threat-source's exercising a specific potential vulnerability, and the resulting impact of that adverse event on the organization [12]. To define the probability of a future adverse event, all threats to an IT system must be analysed in combination with the potential vulnerabilities and the controls in place for the IT system.

Impact refers to the degree of damage that could be caused by a threat's exercise of a vulnerability. The level of impact is governed by the potential mission impacts and in turn produces a relative value for the IT assets and resources affected (e.g., the criticality and sensitivity of the IT system components and data). The risk assessment, implemented throughout the IT system organization for the research project purposes, covers nine primary steps: system characterization, threat identification, vulnerability identification, control analysis, probability determination, impact analysis, risk determination, control recommendations, results documentation [10].

Therefore, at the beginning of the process, it has to be examined, which threat scenarios like force majeure, organisational shortcomings, human failure or software malfunction threaten the IA of classified assets processed during the research activities. Afterwards the decision must be made on how to deal with these risks. The following partial stages are required [9]:

1. Selecting a method for risk assessment.

Possible damage to the classified assets obtained, handled or exchanged within the research project's activities, due to information security incidents must be analysed and assessed. A method for risk assessment is therefore a crucial and integral part of every IA. In order to be able to identify a risk, not only the threats must be recognized and assessed, but also their potential for causing damage and the probability that they will occur. The information security management of the research project must select a method of risk assessment that is appropriate and accepted by each contributing countries NSA [2, 3].

2. Risk assessment.

Every risk assessment must comprise the following steps:

- the information assets and also research processes that are to be protected must be identified;
- all the relevant threats relating to the information assets and research processes that are to be protected must be identified;
- vulnerabilities which the threats can use to take effect must be identified;
- the possible damages due to a loss of confidentiality, integrity or availability must be identified and assessed;
- the assumable repercussions on the research project activities or fulfilment of tasks through IT security incidents must be analysed;
- the risk of suffering damages due to security incidents must be assessed.

3. Classifying risks and damages.

Depending on the selected method for risk assessment, the information security management must determine threats and how relevant influence they can have to classified assets. Also the potentiality of IA damage, occurrence probabilities and the resulting risks should be classified and assessed. Establishing individual values for damages and occurrence probabilities is difficult and in most cases it is more practical to work with categories for both the occurrence probability and potential extent of damages. No more than 3 to 5 categories should be used, for example:

- threat occurrence probability: rarely, frequently, very frequently;
- potential extent of damages or impact level: low, medium, high.

If these kinds of categories have been suitably defined for the research project needs, they can be used as a basis for qualitative risk examination. Table below shows how the overall risk ratings might be determined based on inputs from the threat probability and threat impact categories.

Tab. 1. Risk-Level Matrix [own work]

THREAT PROBABILITY	**IMPACT LEVEL**		
	Low (10)	**Medium (50)**	**High (100)**
R (0.1)	Low 10 x 0.1 = 1	Low 50 x 0.1 = 5	Low 100 x 0.1 = 10
F (0.5)	Low 10 x 0.5 = 5	Med 50 x 05 = 25	Med 100 x 0.5 = 50
VF(1.0)	Low 10 x 1.0 = 10	Med 50 x 1.0 = 50	High 100 x 1.0 = 100
	Risk Scale: High (> 50 to 100), Medium (>10 to 50), Low (1 to 10)		

If an observation or finding is evaluated as a high risk, when the value on the scale will be between 50 to 100, there is a strong need for corrective measures.

An existing system may continue to operate within the research project, but a corrective action plan must be implemented as soon as possible. When the value on the scale is between 10 to 50, the risk level is rated as medium. It means that organizers of the ISMS prepared for the project use, are obliged to implement corrective actions, which must be developed within a reasonable period of time. In case, when a risk is described as low, what means that value on the scale is between 1 to 10, the system's organizers must determine whether corrective actions are still required or decide to accept the risk. When the level indicated on certain items is so low (value is < 1 on risk scale) as to be considered to be negligible or non-significant, there is a possibility to hold these aside instead of forwarding for management action. This will assure that they are not ignored when conducting the next periodic risk assessment and also forms a complete record of all risks identified in the analysis. These risks may move to a new risk level on a reassessment due to a change in threat probability and/or impact and that is why it is critical that their identification not be lost in the exercise [9, 12].

4. Developing a strategy for dealing with risks.

The owner of the risk (manager of the research project) must specify how the identified risks should be dealt with. The personnel responsible for implementation of IA, must accordingly compile information about the risks and choose one of the following options to deal with risk [1, 4, 11]:

- risks can be reduced by implementing appropriate security measures;
- risks can be avoided, for instance, by restructuring or abandoning research processes or tasks;
- risks can be transferred, for instance, through outsourcing or insurances;
- risks can be accepted.

The manner in which risks should be dealt with must be documented and approved by the manager of the research project. The resources necessary for implementing the strategy must be planned and made available.

When developing the strategy of dealing with risk, the residual risk must be also considered as an additional element in the context of the cost planning. The residual risk must therefore be assessed and likewise documented [11].

5. Selecting information assurance safeguards.

Specific information assurance safeguards can be resulting from the general ISMS objectives and requirements. When selecting security measures, the cost-benefit aspects and the practical feasibility must also be considered besides the effects on

the level of information security. Simultaneously with technical information security safeguards, the organisational procedures and processes (such as user guidelines, the granting of rights, security training as well as testing and approval procedures) must also be established. When doing so, the following issues, among other things, must be settled [4, 8]:

- organisation (including specifying responsibilities, assigning duties and separating functions, regulating how information is handled, applications and IT components, hardware and software management, change management, etc.);
- personnel (e.g. briefing new staff members, making deputization arrangements, etc.);
- training and increasing people's awareness on information security;
- data protection (for all information, applications and IT components);
- computer virus protection;
- protection of information during processing, transmission and storage (e.g. through the use of cryptography);
- hardware and software development;
- conduct during IT security incidents (incident handling);
- contingency planning and maintenance of personnel involved in the research project activities in an emergency situation (project continuity);
- outsourcing (e.g. maintenance of hardware).

Comprehensible documentation, explaining why the selected measures are appropriate for achieving the IA objectives and requirements, must be provided. What is more, according to awareness policy, there is not only an obligation to familiarize with these documentation all individuals being users of ISMS, but also all employees of the project have to pass an examination of their knowledge about the rules, principles and responsibilities due to ISMS.

Risk assessment and management is an integral part of IT system live cycle [4]. In fact, above processes thru all stages register to whole process of new classified IT system creation and states as a framework for expected security level IA organization within the research and technology project.

Implementation of IA framework, thanks to the proper risk assessment and management process execution, is important because it provides a road map for the application, evaluation and improvement of information security practices applied in the classified IT system, and what is more, let the security management personnel to articulate goals, evaluate the security of information over time, and determine a need for additional measures if necessary.

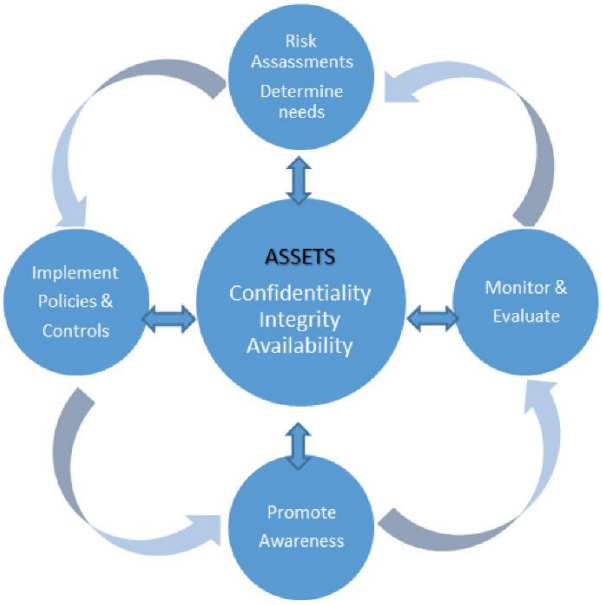

Fig. 1. Basic elements of the risk management cycle [own work]

CONCLUSIONS

The quick access and undisturbed flow of information during the research process is crucial either for the effectiveness of the project management, and also for final results of the researches. IT security become crucial element of each research project due to the fact that all contributors of project are dependent on the IT systems, which have to fulfilled the legal obligation resulting from the fact that majority of the information, generated within the project process, are sensitive and classified. It means that all participating institutions have to implement the proper and unified ISMS procedures and in addition, starting from confidential level of secrecy, applied for Facility Security Clearance (FSC) granted by National Security Authority which is responsible and authorised by multinational agreements in the area of information security for each EU State Member [1, 2]. Within the FSC procedure each participating institution is obliged to pass the classified IT system accreditation, what means the generation of high spending, where costs are resulting, not only from the accreditation procedure but also from the exploitation of IT system. Other problem that occurred during realisation of the researches is enormous amounts of data generated as a working effect of individual researches teams. Diversity of

the analysing systems (different hardware and software solutions), length of the files and access to data base during research process, has indicated the area of problems to solve for the next projects.

Possible solutions, of IT system differences and information exchange difficulties, is to use a potential of cloud computing as a remote platform located in the intranet within the European Defence Agency (EDA), which is the classified research project ordering institution [1, 3]. This resolution let to work the strictly defined group of people, participators to the project, authorised to cloud access in unify security environment. Bearing in mind that cloud provider will pass positively a FSC and IT system accreditation process, the benefits of this resolution are obvious. All participants will work at the same level of classification. Users will have opportunity to work and modify the data to the extent specified in the project assumptions. Every change will generate a record in the history of modified files. The changes are performed instantly and participants have an opportunity to work simultaneously on co-shared files. Additionally, there is no possibility of access to the outdated files reducing the risk of failure during the various project stages. What is more, dynamic access to data on a remote platform eliminates the necessity of documents creation in later versions in case of possible changes in the project. Updating documents in the form of duplication with minor changes causes the accumulation of documentation, what is creating the situation known as data aggregation. From the point of IA view, aggregated data classified as e.g. RESTRICTED shall be protected as CONFIDENTIAL. The use of cloud computing will result in better effectiveness of project management, reliability and infallibility of analysed data and additionally, amounts of classified information will be reduced to necessary minimum, because they will be stored on one properly protected server. And finally, with appropriate organization of the secure access to the cloud, we can minimise the risk of unauthorized individuals access to project assets. Reducing, the risk connected with classified data transportation, monitoring access and 'need to know' principle. All mentioned elements impact directly on IA and cause improvement of information security level within the research project [1].

FSC certification of cloud computing providers is a necessary condition to start implement this resolution for a wider use. All institutions which have been an FSC granted, give a guarantee that they meet the legal requirements and have implemented an efficient Information Security Management System. What is more, applied system is based on internationally recognized standards which are acknowledged and executed by all participants of the process. For the classified information safety, it means that the legal framework applied, gives an assurance of putting into practice

an appropriate resolutions in area of confidentiality, integrity and availability of information which are obtained or exchanged, during a defence and security procurements, by all contributors.

REFERENCES

[1] Buszman K., Listewnik K., Sobczynski T., Sensitive and Classified Data Exchange and Handling in the EU. A Case Study, 'Journal of Information System Security', 2015, Vol. 11, No. 2, pp. 149–168, Information Institute Publishing, Washington DC, USA.

[2] *Council Decision of 31 March 2011 on the security rules for protecting EU classified information (2011/292/EU)*.

[3] *Directive 2009/81/EC of the European Parliament and of the Council of 13 July 2009 on the coordination of procedures for the award of certain works contracts, supply contracts and service contracts by contracting authorities or entities in the fields of defence and security, and amending Directives 2004/17/EC and 2004/18/EC*.

[4] Elsea J. K., *The Protection of Classified Information. The Legal Framework*, Congressional Research Service 7-5700, Washington, 10 January 2013.

[5] *Information Security Risk Assessment. Practices of Leading Organizations*, Accounting and Information Management Division Executive, GAO Guide on Information Security Management, 1999.

[6] ISO/IEC 13335-1:2004, *Information technology. Security techniques. Management of information and communications technology security*, Part 1, *Concepts and models for information and communications technology security management*.

[7] ISO/IEC 27001:2013, *Information technology. Security techniques. Information security management systems. Requirements*.

[8] ISO/IEC 27002:2013, *Information technology. Security techniques. Code of practice for information security controls*.

[9] ISO/IEC 27005:2011, *Information technology. Security techniques. Information security risk management*.

[10] ISO/IEC 27005:2011, *Information technology. Security techniques. Information security management system implementation guidance*.

[11] Monahan G., *Enterprise Risk Management. A Methodology for Achieving Strategic Objectives*, John Wiley & Sons, 2008.

[12] NIST SP 800-30, *Risk Management Guide for Information Technology System, Recommendations of the National Institute of Standards and Technology*.

[13] Taylor A., Alexander D., Finch A., Sutton D., *Information Security Management Principles*, The British Computer Society, 2008.

[14] *The Treaty of Rome*, 25 March 1957.

[15] http://www.eda.europa.eu/info-hub/data-protection [access 27.08.2016]

[16] https://www.enisa.europa.eu/activities/risk-management [access 27.08.2016].

ZASADY OCHRONY INFORMACJI NIEJAWNYCH PRZETWARZANYCH W SYSTEMACH TELEINFORMATYCZNYCH W RAMACH REALIZACJI PROJEKTÓW NAUKOWO-BADAWCZYCH EUROPEJSKIEJ AGENCJI OBRONY

STRESZCZENIE

W artykule zaprezentowano aspekty organizacji ochrony systemów teleinformatycznych wykorzystywanych w ramach systemu zarządzania bezpieczeństwem informacji niejawnych wytwarzanych, przetwarzanych i przechowywanych dla potrzeb realizacji prac naukowo-badawczych Europejskiej Agencji Obrony. Przedstawiono zasady oraz procedury wynikające z uregulowań prawnych normujących przetwarzanie informacji klauzulowanych w systemach teleinformatycznych. Szczególną uwagę zwrócono na zachowanie podstawowych cech sytemu ochrony informacji mających na celu zapewnienie poufności, integralności oraz dostępności informacji wytworzonych w trakcie realizacji procesu badawczego.

Słowa kluczowe:

informacje niejawne, informacje wrażliwe, bezpieczeństwo teleinformatyczne, ocena ryzyka, szacowanie poziomu zagrożeń, akredytacja, certyfikacja, przetwarzanie i przesyłanie niejawnych materiałów UE.