Sekulovska-Jovkovska, Ana; Mitrevski, Pece; Arsenovski, Sime

Article

Preventing corrupt practices in public institutions in the Western Balkans: Application of ICT security standards, policies and procedures

UTMS Journal of Economics

Provided in Cooperation with:
University of Tourism and Management, Skopje

Suggested Citation: Sekulovska-Jovkovska, Ana; Mitrevski, Pece; Arsenovski, Sime (2020) : Preventing corrupt practices in public institutions in the Western Balkans: Application of ICT security standards, policies and procedures, UTMS Journal of Economics, ISSN 1857-6982, University of Tourism and Management, Skopje, Vol. 11, Iss. 1, pp. 67-79

This Version is available at:
https://hdl.handle.net/10419/281873

Ana Sekulovska–Jovkovska, Pece Mitrevski, and Sime Arsenovski. 2020. Preventing Corrupt Practices in Public Institutions in the Western Balkans: Application of ICT Security Standards, Policies and Procedures. *UTMS Journal of Economics* 11(1): 67–79.

Original scientific paper
(accepted September 04, 2020)

PREVENTING CORRUPT PRACTICES IN PUBLIC INSTITUTIONS IN THE WESTERN BALKANS: APPLICATION OF ICT SECURITY STANDARDS, POLICIES AND PROCEDURES

Ana Sekulovska – Jovkovska[1]
Pece Mitrevski
Sime Arsenovski

Abstract:
Information security (INFOSEC) seeks to integrate previously distinct disciplines such as: employee security, computer security, communications security and operational security. It is ensured by an appropriate set of controls, which can be principles, practices, procedures, organizational structures, and software functions. The ISO/IEC 27001 standard is subject to different areas of application as well as differentiation of possible processes in the organization that are related to the management of security control such as: security policy, security of the organization, control and classification of the source, security of employees, security of tangible assets and environment, operational management and communications, access control, development and maintenance of various systems, and continuity management. We address the following areas: information security, ISO/IEC 27001 standard and provide some negative examples from countries in the WB6 region where the abuse of IT systems took place due to non–compliance, i.e. the lack of minimum security standards necessary for safe, quality and systematic operation in public institutions. It is necessary to create a national strategy that should list short–term, medium–term and long–term measures that need to be taken and implemented in order to follow the security IT standards and trends in countries where this type of standards and measures are applied and give appropriate results.

Keywords: computer security, information security, standardization, corrupt activities.

JEL classification: K42; K24; F52

INTRODUCTION

The term information security was coined in the United States on the basis of information warfare (IW). In the words of Daniel Wolf (Wolf 2013), historically, communication security (COMSEC) first appeared in the 1960s. With the advent of computers in the 70's, computer security (COMPUSEC) appeared. In the late 1980s,

[1]**Ana Sekulovska Jovkovska,** Ph.D., Assistant Professor, Faculty of Informatics, University of Tourism and Management in Skopje, Republic of North Macedonia; **Pece Mitrevski,** Ph.D., Full Professor, Faculty of Information and Communication Technologies, University "St. Kliment Ohridski" – Bitola, Republic of North Macedonia; **Sime Aesenovski,** Ph.D., Full Professor, Faculty of Informatics, University of Tourism and Management in Skopje, Republic of North Macedonia.

COMSEC and COMPUSEC merged into information security (INFOSEC) which sought to integrate previously distinct disciplines such as: employee security, computer security, communications security and operational security. INFOSEC focuses on preventing unauthorized access to information systems. Confidentiality, integrity and availability of information were considered first. In the past, information security has been defined as: "protection of information systems against unauthorized access or modification of information whether in storage, processing or transmission and against deprivation of services of authorized users, including necessary measures to detect, document and repel such threats" (NSA, 1992).

With the advancement of computer technology and the advent of networks (LAN and WAN and above all the INTERNET) the list of information properties, before which security requirements are set, is expanding. These are authentication and non–repudiation. Based on the stated properties of information (or information security services and information systems), the term Information Assurance (IA) was coined in the 1990s. It is important to note that the difference is not only of a terminological nature, but that it is a matter of substantial change. In addition to the listed security services, the information guarantee has another important features: operability and time sensitivity. This characteristic is expressed by the terms detection and reaction. The word is in the defensive operational capabilities which, together with the traditional IA activities, in the late 90's describe the term Information Warfare Theory – Defense Information Operations (DIO) (Wolf 2013; Department of the Army 2003).

Finally, in 2002, under the direction of the US Department of Defense (DODD number 8500.1 information assurance, October 2002), the term information guarantee was officially introduced when it was defined as information operations protection and defense of information and information systems, ensuring their availability, integrity, authenticity, confidentiality and indisputability. This means restoring the information system, incorporating protection, detection and response capabilities. When it comes to information security in the United States, there is close cooperation between the public and private sectors, as defined in all documents. European countries in their understanding of the term Information Security with a pronounced pragmatic approach follow the views of the United States (Luiijf 1999), whereas the consideration of the term Information Security in the Russian Federation is of a more recent date (from the 90's): according to some authors (Panarin 1997) the former USSR lost the Cold War due to neglect of information security in the information sphere of society.

In the Republic of North Macedonia, the term information security is not sufficiently considered. The terms information protection, security and information protection or data protection address some of the aspects of information security. The fact that according to the modern interpretations of the term national security, information security is one of its basic components, makes the issue of information security extremely relevant. The remainder of this paper is organized as follows. Section 1 introduces the concepts of Information Security (IS) and Information Security Management Systems (ISMS). Section 2 is devoted to standardization and the ISO/IEC 27000 standard. Some typical examples of corrupt activities of public sector employees

in the Western Balkan countries are disclosed in Section 3, whereas in the concluding section we summarize all of the above in order to help build quality, safe, responsible public institutions that will be completely in the service of the citizens and will work for the good of the state.

1. INFORMATION SECURITY CONCEPTS

There are many different definitions and interpretations of the term information, but as one of the many interpretations we will mention the definition of the term in the business world: information is a property like other important business properties necessary for the business of the organization, so it must be properly protected. This is very important in an increasingly interconnected business. As a result of growing mutual values, information is now exposed in increasing numbers and with a wider range of threats and vulnerabilities. Whatever the shape:

- written documents (documents, archives, letters, documents, reports, etc.),
- electronically stored (on a network, on servers, computers, laptop, USB, CD, DVD, etc.),
- transmitted information (Email, http, ftp, download, peer to peer, etc.),
- showing video material (video surveillance, public and private video, recordings, etc.),
- conversations (telephone, public, IP telephony, etc.)

in which they are located, or on the means by which they are distributed and nourished, should always be adequately protected.

The abbreviation CIA (Confidentiality–Integrity–Availability) (Chapple 2020) for information security is:

- Confidentiality (confidentiality), ensuring that information is only accessible to those who are allowed access,
- Integrity – means preserving the accuracy and completeness of information and processing method,
- Availability – ensuring that authorized users have access to the information and property associated with it when required.

Figure 1. CIA Information Security Overview

Information security is ensured by an appropriate set of controls, which can be principles, practices, procedures, organizational structures, and software functions. These controls need to be in place to ensure compliance with the organization's specific security objectives.

In the modern connected world, information and related processes, systems and networks are critical business properties. Organizations and their information systems and networks are often exposed to security threats from a wide variety of sources, including computer fraud, espionage, sabotage, vandalism, fires, and floods. Threats to malicious information systems and networks, hacking, and denial–of–service attacks are becoming more common, more ambitious, and more sophisticated. The Information Security Management System (ISMS) provides a model for establishing, implementing, using, supervising, auditing, maintaining and enhancing information protection, in order to achieve business objectives, based on the assessment of risk and levels that are acceptable for risk in the organization (Ibnugraha et al. 2020). ISMS must safeguard the information security interests and needs of all stakeholders, including buyers, suppliers, business partners, co–owners and other relevant parties.

The complete transition of electronic data processing, the strengthening of electronic commerce and the large number of channels for data collection and distribution affect the increase in the number of security incidents. Through the information contained in the information system of the organization often represent business secrets that are essential for the company.

- Example 1. If the flow of information in the company is disabled, how long would it function?
- Example 2. Unconsciously using incorrect data. How can you make strategic and operational decisions based on them?
- Example 3. The data in the company can be accessed by anyone, even the competition. How much future would that organization / company have?

The answer to all the above questions is primarily given by the Information Security Management System, which is created on the series of standards ISO/IEC 27000. Effective operation is based on the identification and management of a range of activities. The term process is the management of a series of activities that use resources to transform input and output. The application of the system of processes in the organization, with the identification and interaction of those processes, as well as their management is called the process approach.

The ISMS process approach according to this set of standards is based on the principle that is unique to all ISO systems management standards: Plan–Do–Check–Act (PDCA).

- Plan – to create goals and plans (analyzing the situation, setting goals and developing plans to achieve the goals)
- Make – implementation of plans,
- Check – measure the results (how many plans have been realized)
- Act – correct and improve activities (learn from mistakes to achieve better results)

2. STANDARDIZATION: WHAT IS ISO/IEC 27001?

The ISO/IEC 27001 standard (International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) 2013a) is part of a series of ISO/IEC 27000 standards, which aims to ensure the availability, confidentiality and integrity of data by establishing mechanisms for their control and protection. Today, when all the work in an organization is performed through IT systems, data security is extremely important. Due to the existence of threats from different sources, it is necessary to take measures to protect them. Nowadays, in conditions of market competition, providing timely and reliable information is a condition for the success of a company or organization. Users need information that is up to date, secure and timely.

ISO/IEC 27001 is a standard for information protection and security. The standard is subject to different areas of application as well as differentiation of possible processes in the organization that are related to the management of security control such as: security policy, security of the organization, control and classification of the source, security of employees, security of tangible assets and environment, operational management and communications, access control, development and maintenance of various systems, and continuity management. This series covers standards that: define ISMS requirements as well as requirements for ISMS certified bodies, provide support, detailed guidance and instructions for the entire Plan–Do–Check–Act process, provide specific sector guidance for ISMS and ISMS compliance assessment.

The standard covers companies of all sizes (small, medium and large), all forms of regulation (public and state sector, private companies, NGOs), as well as all types of industries, i.e. areas of operation (banking, manufacturing, IT sector, utilities, health, state institutions, security services, etc.). The goal of all of them is to keep the information identical and for all employees to know the precise steps in order to protect the data available to their organization. ISO 27001 requires a certain way of monitoring and management of IT systems which primarily refers to:

- Systematic, organized and planned reviews of security risks for organizational information,
- Taking into account the potential threats and vulnerabilities of the IT systems, as well as the consequences of the intrusion into the system, i.e. the harmful effects of the company itself,
- Design and implement comprehensive packages of security controls on the company's sensitive information,
- Implement a security risk response strategy to protect information in a timely manner,
- Constantly checking and improving the process of security control of sensitive data so that the system would remain secure and resistant to new threats, in order to provide additional protection and prevent unauthorized use of information,

- Ensuring continuity of work (back up systems, redundancy of vital parts of the IT structure, disaster recovery plan)

A top–down approach to risk analysis is used where the requirements are technologically neutral, i.e. do not depend on any applied technology. The certification defines planning consisting of six steps:

1. Defining security policies
2. Defining the scope of ISMS
3. Risk assessment
4. Identification of risks
5. Selection of control facilities and control to be implemented
6. Preparation of a statement of applicability

Organizations that are aware of information ownership recognize the information assets they own and are aware of their value. They undertake to protect their property by using methods of protection, establishing appropriate control by a precisely established procedure. This awareness leads to the introduction of the ISO/IEC 27001 standard which leads to the protection of the reputation of the organization, avoids damage, saves funds, reduces risks and more. By accepting the standard and setting up effective processes in the organization, a clear message is given to customers, employees and other and third parties that the internationally recognized practice of information security is being used. The main advantages of introducing ISO 27001 (TÜRCERT 2018) are the following:

- Employees create data protection awareness
- The reliability of information is continuously assessed
- System performance improves due to regular monitoring
- Information security activities are supported by process control and documentation creation
- As the information system and computer networks will be continuously monitored, the system will be constantly protected from computer threats and dangers.
- The importance of data protection in the organization will be presented
- It will be proven that information ownership protects against violent attacks and malicious uses
- Data confidentiality is created

With the introduction of ISO/IEC 27001, it provides customers and associates with confidence in your information system, the way of risk management, as well as the way of working that makes a positive reputation and distinguishes itself from the competition. A systematic approach and standard procedures take precedence to identify information security threats and create plans to address them. This process can be managed and risk exposure reduced, leading to a secure exchange of information. The implementation of the standard develops awareness among employees about the importance of information as a key resource in the work, but at the same time responsibility for information security by all employees and at the level of the entire organization. With the introduction of the information security system helps us to meet

the requirements of various data protection laws. By reducing the risk of damage, loss and misuse of information leads to small costs per organization and thus increased profitability. Working with processes that are based on the principle of security allows better cooperation with organizations around the world that work on the same model. With the introduction of the standard, an advantage is achieved in obtaining things that involve working with confidential data.

3. CORRUPT ACTIVITIES OF PUBLIC SECTOR EMPLOYEES IN THE WESTERN BALKAN COUNTRIES

3.1 North Macedonia

In the Republic of North Macedonia, in 2010, the Ministry of Interior received a series of information after which a series of police measures were applied, which confirmed most of the information and opened a police investigation related to abuses committed by toll employees, i.e. employees of the Public Enterprise for State Roads of the Republic of North Macedonia (Stoilkovski and Stojova 2013). The detailed investigation has established that in this case it is a combination of various types of abuse of the information system committed by employees, as follows:

- Abuse of the information system by using various authorizations for authentication in the system and frequent use of authorizations for authentication of other employees,
- Giving approvals for release of vehicles without settling the costs for using the toll,
- Entering the information system by changing the amount that was paid,
- Failure to register all vehicles that passed the toll,
- Non–issuance of fiscal invoices and sharing of the amount with the driver of the vehicle on a 50:50 basis,
- Entering another category of vehicles in the system instead of the one that really passed through the toll.

Through various analyzes of the previously provided information from the engaged services, data from the information system were taken, anomalies in the way the system works in the organization were accurately detected, an assessment was made in order to calculate the damages that were done for the period. The entire investigation shows that this is an abuse committed by persons employed in the public enterprise in various positions, in their official capacity they used the information system, which enabled the employees to gain illegal profit which, at a later stage, was "laundered" through legal investments in other goods. After the completion of this case, the management of the public enterprise that manages the tolls in the Republic of North Macedonia is obliged to improve the information system for managing the procedure for payment of tolls and for monitoring the manner of work of the employees.

3.2 Serbia

In the Republic of Serbia, in May 2007, the trial of the so–called "road mafia" began, which involved a total of 53 people, most of them employees of the public company "Putevi Srbije" (Nenadic and Cvetkovic 2013). In the part of the description that can be obtained from the investigating authorities, this investigation is described as the biggest robbery using electronic tools in the history of the Serbian judiciary.

With the help of inserting additional hardware (inserting additional cable connection of devices) and software add–ons (inserting a corrupt copy of the software tool of the electronic toll collection system of the existing operating system which had a different function and purpose), parallel operation was performed of the toll collection system at two most frequent locations ("Bubanj Potok" and "Nais" (both ends of the highway Nis – Belgrade)) which enabled the shift manager to start the illegal program before the start of the shift, which together with the additional hardware enabled the persons who collect the toll (members of the organized group) to simultaneously print two bills for toll with the same serial numbers and to record only one of them in the system. When the toll was paid on the basis of this double bill, the software allowed the bill to be printed without registering it in the electronic toll collection system. At the same time, by pressing a special button (the button interrupted the connection between the electronic payment control system, the computer and the ramp), the trucks were allowed to continue their journey after the payment was made. The fraudulent system has been operating for a much longer period of time and the investigation has covered only some of its aspects and perpetrators.

3.3 Montenegro

The case in the Republic of Montenegro refers to the electronic preparation of false permits and other certificates in order to use such permits in legal proceedings (Drakic and Lazarevic 2013). Two persons used their position and function to gain illegal benefit and exceeded their official powers because they drafted and published decisions for which they did not have the authority to draft. With the first decision they drafted, they enabled the return (restitution) and transfer of state land to a person who allegedly owned that land before. This person registered the land in the electronic cadastre and immediately sold it. At the same time and in the same way, the defendants issued another decision with false content, by which some land was returned to a person who allegedly previously owned that land. In this case, immediately after the illegal registration, the alleged owner immediately sold the land, although he did not have a valid property certificate, with the help and signature of the accused officials. By performing and enabling such activities and through land restitution, the defendants gained financial benefits in the amount of about 570,000 EUR.

3.4 Albania

The example of the Republic of Albania refers to the abuse of police stations at border crossings committed by border police officers, by manipulating TIMS information systems (TIMS – Complete Information Management System) in order to avoid charges to the state for import of vehicles (Nasi and Kercini 2013).

The person who owns a motor vehicle, through a special power of attorney, gave the right to another person to use a vehicle with Italian license plates. With this document, the user of the motor vehicle is given the legal right to act and apply to the relevant institutions for full procedure and registration of the vehicle that was imported, and to go through the appropriate procedures so that the vehicle can be used freely and legally in Albania.

As of March 1, 2012, biometric passports are the only valid passport for Albanian citizens, all border crossings use biometric passport readers and fingerprint checking equipment. Recording the documents in real time and reading them at the moment of entry and exit at the border crossings enables comparison with the existing data and reduces the probability of fraud. The intervention on the system was made by a person employed at a border crossing who from May 1, 2010 worked as a system operator. In this position he participated in the control of persons and vehicles and in the registration of entry and exit to and from Albania. The prosecution filed criminal charges against the sparrow at the border crossing point for making false changes in the system and acting against the public interest, by preparing a false report that refers to the user of the vehicle.

3.5 Kosovo

In the period after the wars in Kosovo, there are many demands for the final stabilization of the situation and work towards the well–being of the citizens, by creating new jobs and providing conditions for the overall development of the country (Preteni and Elsani 2013). One of the priorities of the Government in that period is the improvement of the road infrastructure and significant financial resources have been allocated for the construction of local and regional roads.

State officials began to demand bribes from any company seeking a work contract – the amount required for each contract varied between 10% and 20% of the total tender value. Since its inception, the Anti–Corruption Agency has received information on numerous allegations of corruption in this field. The most specific complaint was submitted by the owner of a company in which he complained that, in order to obtain a contract worth millions, the civil servants demanded a high amount of bribe (seven digits, i.e. 15%) of the total value of the tender. All the material that the investigators expect to find has been deleted from the Government's servers, which would confirm the suspicions of the Anti–Corruption Agency for irregularities and violations of the law. In order to prevent similar scams in the future, the servers could be placed under some kind of independent control.

3.6 Bosnia and Herzegovina

The Citizens' Identification Data Protection System (CIPS) project started in Bosnia and Herzegovina in April 2002, when a directorate was set up to implement it on a temporary basis (Martinovic and Nogo 2013). The main task of the project is to establish a special part of the system that will enable the implementation of the Law on Central Registers and data exchange. In 2008, in accordance with the Strategy for Development of Identification Documents, this Directorate became the Agency for Identification, Registration and Data Exchange (IDDEEA) of Bosnia and Herzegovina.

From the very beginning of the Project for system of protection of citizens' identification data, numerous complaints have been registered regarding the abuse of its electronic system, especially when it comes to issuing ID cards and passports at the national level. Some of the public officials are suspected of being involved in organized crime by abusing their financial and technical resources, thus allowing entire organized groups to illegally gain material benefits. Police officers used their official computers and access rights to log in and exchange data. Namely, they would find a certain person in the database who had the citizenship of Bosnia and Herzegovina but who was never issued an ID card (for example, refugees who went abroad during the war and never returned). The person who wanted to obtain forged documents would then be sent to the registrar's office (otherwise part of an organized crime group operating under the auspices of the municipal administration) who would issue him a birth certificate and a citizenship certificate under a false name, which is considered sufficient to initiate the procedure for issuing an ID card. In some cases, data from deceased persons were even used: instead of officially registering that a particular person had died, they would register the person who had lost a valid ID card as lost and initiate a procedure to issue a new identity card.

These illegally obtained personal documents were to a significant extent used for criminal activities in various parts of the country and in the region. This major case was causing enormous damage to the reputation of public services across the country and as a result, several changes in procedures have been initiated to prevent similar cases in the future.

3.7 Regional summary

Western Balkan countries are signatories of all the related Council of Europe agreements, enabling the provisions for those to become part of the domestic legal systems. Since all the countries are on the EU track, there is a formal follow–up on implementing the EU requirements as well, both on a policy and on an operational level. Table 1 summarises the status of development of the key cybersecurity elements of the national environment in each of the countries of the Western Balkans: "+" denotes that (at least) the basics are in place, "–/+" denotes that some early developments are on the way, while "–" denotes there are no significant developments

identified (DiploFoundation 2016; RSh 2014; BIH 2019; RKs 2020; RNM 2018; GoM 2017; RS 2010).

Table 1. Cybersecurity environment in the Western Balkans

	ALB	BIH	KOS	MKD	MNE	SRB
Cyber Security / Information Security Law	–/+	–	–	–	+	+
Cybercrime (in) Law	+	+	+	+	+	+
Cyber Security / Information Security Strategy	+	–/+	+	+	+	–/+
National Computer Emergency Response Team	+	–/+	+	+	+	+
Substantial Public–Private Partnerships	–/+	–	–/+	–	–/+	–
Confidence Building / Education	–	–/+	–	–	+	–

CONCLUSION

We aimed to address the following areas: information security, ISO/IEC 27001 standard and provided some negative examples from countries in the region where the abuse of IT systems due to non–compliance, i.e. the lack of minimum security standards necessary for safe, quality and systematic operation in public institutions took place. From all this, it can be concluded that security is a very important segment of today and should not be neglected. If, as a country, we want to have public institutions that will meet the security standards that are the practice in highly developed countries, it is necessary to show the readiness of institutions and organizations to successfully deal with all security threats. ISO/IEC 27001 itself is a standard that is atypical in terms of management systems. The basic part of the standard contains relatively few requirements, but Annex A is very extensive and thorough. Complete implementation of the standard requires at least one year of intensive work, and the application is impossible without the involvement of the IT sector. The application aspects are technical, organizational and combined. The documentation required is very extensive and the verification procedure is very detailed. A very important segment in the overall implementation is the training of employees and the development of their awareness for information protection, in order to successfully implement the system and identify potential problems. Annex A itself contains a total of 133 controls that do not refer only to IT control, but also cover physical security, legal protection, human resource management, organizational issues and more. Thus, Annex A can be considered as a catalog of security measures used during the review of the risk procedure, when unacceptable risks are identified in the risk assessment procedure. Annex A helps us to select a measure/measures/ control/controls. which will reduce such risks, but also prevent any important controls from being missed.

When we summarize all the above, and if we feel the need to build quality, safe, responsible public institutions that will be completely in the service of the citizens and

will work for the good of the state, it is necessary to create a national strategy that will be designed for an exactly defined period: it should list short–term, medium–term and long–term measures that need to be taken and implemented in order to follow the IT security standards and trends in countries where this type of standards and measures are applied and give appropriate results.

REFERENCES

Bosnia and Herzegovina. 2019. *Cybersecurity Capacity Review*.

Chapple, M. 2020. *Confidentiality, integrity and availability – The CIA Triad*, https://www.certmike.com/confidentiality–integrity–and–availability–the–cia–triad/, [accessed April 2020].

Department of the Army, Field manual No. 3–13, FM 3–13(FM 100–6) *Information operations: Doctrine, Tactics, Technigues, and Procedures*. Washington, DC, November 2003, https://fas.org/irp/doddir/army/fm3–13–2003.pdf, [accessed April 2020].

DiploFoundation. 2016. *Cybersecurity in the Western Balkans: Policy gaps and cooperation opportunities*. Geneva: DiploFoundation.

Drakic, D., and I. Lazarevic. 2013. *Abuse of IT for Corruption*: 72–73. Danilovgrad Montenegro: ReSPA.

Government of Montenegro, Ministry of Public Administration. 2017. *Cyber Security Strategy of Montenegro 2018-2021*.

Ibnugraha, P.D., L.E. Nugroho, and P.I. Santosa. 2020. Risk model development for information security in organization environment based on business perspectives. *International Journal of Information Security*. https://doi.org/10.1007/s10207-020-00495-7

International Organization for Standardization (ISO), and the International Electrotechnical Commission(IEC). 2013a. *ISO/IEC 27001: Information Security Management*, https://www.iso.org/isoiec–27001–information–security.html, [accessed April 2020].

Luiijf E., *Information Assurance and the Information Society*, EICAR Proceedings 1999.

Martinovic, A., and S. Nogo. 2013. *Abuse of IT for Corruption*: 35–37. Danilovgrad Montenegro: ReSPA.

Nasi, E., and E. Kercini. 2013. *Abuse of IT for Corruption*: 21–23. Danilovgrad Montenegro: ReSPA.

National Security Agency, *National Information Systems Secutity Glossary*, NSTISSI No 4009, http://www.tscm.com/nstiss.html, [accessed April 2020].

Nenadic, N., and B. Cvetkovic. 2013. *Abuse of IT for Corruption*: 86–88. Danilovgrad Montenegro: ReSPA.

Panarin I. N. 1997. *Problems of lack of information security in modern conditions* [Проблемы обеспечения информационной безопасности в савременных условиях], http://kiev–security.org.ua.

Preteni, H., and D. Elsani. 2013. *Abuse of IT for Corruption*: 52–54. Danilovgrad Montenegro: ReSPA.

Republic of Kosovo. 2020. *Cybersecurity Capacity Review.*

Republic of North Macedonia. 2018. *National Cyber Security Strategy 2018-2022 and Action Plan 2018-2022.*

Republic of Serbia. 2010. *Information Society Development Strategy in the Republic of Serbia until year 2020.*

Republika e Shqipërisë, Ministria e Mbrojtjes. 2014. *Strategjia për Mbrojtjen Kibernetike (Cyber Defense).*

Stoilkovski, M., and R. Stojova. 2013. *Abuse of IT for Corruption*: 59–60. Danilovgrad Montenegro: ReSPA.

TÜRCERT Tehnička kontrola i certifikacija ISO 27001. 2018. *Sustav Upravljanja Sigurnoscu informacija*, https://www.sertifikasyon.net/hr/detay/iso–27001–bilgi–guvenligi–yonetim–sistemi–faydalari–nelerdir/, [accessed April 2020].

Wolf, Daniel G. 2003. Statement before the House Select Committee on Homeland Security Subcommittee on Cybersecurity, *Science and Research & Development*, National Security Agency US.