Contents lists available at Science-Gate

International Journal of Advanced and Applied Sciences

Journal homepage: http://www.science-gate.com/IJAAS.html

Using banking information security management to ensure system stability and investors' well being

Ioana Carmen Rada, Ioan Constantin Rada *

Department of Engineering and Management, Faculty of Electrical Engineering, University of Oradea, Oradea, Romania

ARTICLE INFO

Article history:
Received 17 May 2017
Received in revised form
22 October 2017
Accepted 15 November 2017

Keywords:
Security
Information security
Banking Information
Information security management
Ensuring information security

ABSTRACT

In order to carry out our research, we use the case study method, one of the various existing research methods, with its advantages and disadvantages. We preferred this strategy because the initial questions we addressed are: "how" and "why" and because we have little control over the events, and our attention is directed to the phenomenon: "The need to modernize banking security along with prudential supervision in order to protect the interests of depositors and to ensure the stability and viability of the entire banking system in the National Bank of Romania", in order to eliminate this phenomenon by "Modernizing the historical methods of prudential supervision of credit and security institutions in the European context through managing the security of banking and prudential supervision to protect the interests of depositors and the stability and viability of the entire banking system." We use this method because we intend to deal with the contextual conditions of the need to modernize prudential supervision and banking security in order to protect the interests of depositors and to ensure the stability and viability of the entire banking system in the National Bank of Romania in the belief that they can be particularly relevant to the phenomenon studied. The need for modernization is generated by the financial and banking crisis that started in 2008, and this is done through the banking information security management, along with the modernization of prudential supervision of bank and non-bank credit institutions.

1. Introduction

Information, as independent element of the informational system of any organization's management, including banks, consists of data which produces an increase of knowledge that in turn concerns, either directly or indirectly, a certain organization, which provides new elements, useful in fulfilling its needs.

In order to function properly, any organization needs resources. These may be either visible - material, financial, human, capital (fixed), or invisible - information resources. Some authors have divided the last century into the industrial society and the post-industrial, or informational society. It's known that, within an industrial society, the crucial production is the industrial one and the strategic resource is represented by capital. However, at the core of the Information Society is the intellectual production, and information has become the most important resource. With information as strategic resource, the economic system has been reached much easier.

Of course experts have pointed out at the differences between information, data and knowledge, but at the same time, with all the differences and connections between them, which contribute to the generation of information systems. Thus, Argyris (1992) has shown that data is composed from primary elements, collected for information purposes or in order to solve problems (Argyris, 1992). For other authors (Miranda, 1984), "The concepts of information and data are considered synonymous in everyday speech", but in reality they are essentially different. Economists, engineers, managers or businessmen have to understand the concepts they work with.

As in any scientific system, there are basic notions on which the information system is built. Information is a basic concept (Clifton, 1990; Benyon, 1990; Lucey, 1991), and the notion of data derives from it. However, if one starts from the hypothesis that data is the basic notion (Watters, 1992), the concept of information is the derived

* Corresponding Author.
Email Address: ioana.rada@bnro.ro (I. C. Rada)
https://doi.org/10.21833/ijaas.2018.01.007

notion. However, there are more complete definitions. In this regard we find, in one of the most prestigious specialized dictionaries, the following explanation: "formally, a collection of symbols. This is the meaning of information processing, information technology or information theory. The symbols are defined as means whereby meaning is retained and thus they serve as an alternative definition of information".

Information is also defined by three essential aspects: syntactic, semantic and pragmatic; the most concrete aspect of information is the pragmatic one, as it relates information to the observer's purposes.

While being aware that, in banking, information and data may be used as synonyms only by an agreement according to which the object should be used as its model, taking into account that economic and business information are rather pragmatic concerns, that there are many controversies between philosophers, computer scientists, cyberneticists and others on this issue, and also that research in this area is unlimited, our approach focuses only on a few issues regarding the use of databases referring to the Credit Risk Register and the Payment Incidents Register. We find that an important issue in this respect is to create a public system for the management and report of loan and payment incident information.

Thus, Gabriela et al. (2015) argued that "The creation of public reporting and credit information management systems, in the form of central and private credit registers, as credit bureaus, came to respond to more and more pressing demands in this respect, both at micro and macro-prudential levels. If private credit bureaus respond to particular requirements of creditors to reduce credit risk in their own activity, central credit registers satisfy the additional needs of central banks in exercising their role of regulators and supervisors of the banking system". The categories of credit information hold, their structuring levels and detail, the services offered, make the two types of credit information management systems complementary, each bringing added value to users.

Specific information regarding credit risk, cards frauds, individual risk, the overall risk and many other concepts, useful forms and information flow are governed by NBR (2012b) of January 9th 2012, published in the Official Gazette, Part I 49, in January 20th 2012, which become operational on February 1st 2012, on the organization and functioning, within the National Bank of Romania, of the Credit Risk Register, amended and supplemented.

Information specific to payment incidents and public interest, including users' specific goals, are governed by NBR (2012a) of January 9th 2012 published in the Official Gazette, Part I 49, in January 20th 2012, which become operational on February 1st 2012, on the organization and functioning, within the National Bank of Romania, of the Credit Risk Register.

2. Concepts regarding the safety and the security of banking information

The question is whether financial and banking information security management can be ensured against the Black Swans, uncertainties and risks and at the same time, and achieves its goals. The metaphor of the Black Swan, which is widely used nowadays, explains how these go beyond the logical and philosophical question and enter the empirical reality: "I employed the logical metaphor of the black swan (lowercase) for Black Swan events" (Taleb, 2010). The author just mentioned states that this should not be confused with the logical problem raised by many philosophers. "It does not refer to exceptions, but to the oversized role of extreme events in many areas of life. The Black Swan refers to the role of exceptional events that lead to the degradation of predictability and the need to resist negative Black Swans and exposure to the positive ones' (Taleb, 2010).

Managers are aware of and will be able to apply their managerial mechanism in the triad: Fragile-Robust-Ant-ifragile for making decision regarding banking information security. The concept of triad belongs to the same Nassim Nicolas Taleb, an expert on risk, uncertainty and probability in economy (Doina and Constantin, 2016). "The anti-fragile is a guide to living in a world that we don't understand, dominated by Black Swans and the human obsession for the predictable and the safe" (Taleb, 2014). Erudite, witty and bold, Taleb's message is revolutionary: "Only the anti-fragile will survive."

Throughout human existence, the need for stability became obvious, along with the demand for ensuring economic security, labor organizations in various forms etc. The concepts of security and stability arise from the modern approach to the definition of security. Regulations that are functional in Romania (Law no. 51/1991) define the concept of security as "the state of legality, balance and social stability, economic and political [...]". International organizations, such as the United Nations (Charter), NATO and the Organization for Security and Co-operation in Europe (O.S.C.E.) define the concept of security. For example, the definition given by O.S.C.E is presented in the Charter for European Security: "Each participating State has an equal right to security. We reaffirm the inalienable right of each participating State, and of all the states participating, to the freedom of choosing their own security commitments, including treaties of alliance, as they are issued. Also, each state has the right to neutrality. Each participating State will respect the rights of all the others thereon. They will not strengthen their security at the expense of other countries' security [...]". According to some authors (Ţigănoaia, 2013) it can refer to several aspects, as shown in Fig. 1. In this approach we refer to organizational security (bank) or alternatively, to security bank information.

The reference to the security of some entity (organization, institution, person, system, etc.) can lead us to think of a number of means for ensuring

all the conditions so that the entity should be able to meet all the objectives for which it was created.

In accordance with the concepts of the National Center for Response to Security Incidents in Information Systems (CERT-RO) of the Ministry of Communications and Information Society, concerning: Risk Management, Security incidents, vulnerabilities, countermeasures", information is secure when availability, confidentiality, integrity, authenticity and non-repudiation are fully ensured to the extent that is necessary for the entity that created it, or the one that uses it."

Fig. 1: Aspects related to the security concept (Ţigănoaia, 2013)

Moving on to analyze the objective of this work we shall refer to the security of "credit risk information and information about card fraud, for the specific purposes of users, in terms of professional secrecy" (NBR, 2012b). We analyze here the security on the CRR participation to "cross-border exchange of information in accordance with the Memorandum on the exchange of information between national credit registers, with the view of transmitting such information to reporting entities, concluded by the National Bank of Romania with the competent authorities in the Member States' (NBR, 2012b). In this situation the management of banking information security refers to the database organized and managed by CRR. This database includes:

a) The Central Credit File (CCF), which contains information regarding credit risk reported by entities, processed and disseminated by the CRR in order to be employed by users under the conditions of professional secrecy;
b) The Overdue Debt File (ODF), which is fed, by CCF, on a monthly basis, with information on credit risk on borrowers and their overdue loans to all reporting entities in Romania;
c) The Groups File (GF) that is fed monthly by CCF with information about groups;
d) The Card Fraud File (CFF), which contains information on card frauds committed by holders of credit cards and/or credit "(NBR, 2012b).

In regards to the security of database access, "reporting entities shall designate up to 5 people accredited to CRR" (NBR, 2012b), and "the informatics system of the CRR is to be accessed only by CRR accredited persons", based on a name given by the National Bank of Romania.

The security of sending and recording credit risk information and information about credit card fraud must follow a certain regimen. The security of disseminating credit risk information and of information about credit card fraud, held by CRR, should be implemented in "the CRR information flow." The security of correcting information erroneously forwarded to CRR must be ensured during the reporting period, and the security of correcting information recorded in the CRR database constitutes an earlier reporting that can be done by the reporting person with the help of certain forms. The accuracy of data recorded in the database of CRR can be challenged by a debtor, without knowing the reporting person - the source of the error, asking the reporting entity that has submitted information for credit risk and/or information about card fraud, to start, only one time, the conciliation procedure.

The other objective of our research refers to the security of information specific to payment incidents, for public interest, including for the specific purposes of users. The concept of security and safety of this type of banking information extends to the PIB (Payment Incidents Bureau) database structure and access to it. The PIB organizes and manages the database and its security, comprising:

a) The Payment Incidents National File, called PINF, which is a general interest file containing payment incidents with checks, promissory notes, bills of exchange and is structured as follows: Checks National File (CNF); National File Bills (NFB); National File of Promissory Notes (NFPN);
b) The National File of People at Risk (NFPR), contains major payment incidents registered in the name of individuals or legal entities, resident or nonresident, and is powered automatically by PINF" (NBR, 2012a).

At the same time, it is extremely important to ensure access to databases, thus "reporting entities are required to designate up to 5 persons accredited to the PIB. To this end, they should complete and update the form". The accreditation of persons at the PIB, authorized to transmit and receive information on payment incidents" (NBR, 2012a). Then we talk about the security of access to the information system at the PIB. This access is based on names awarded by the National Bank of Romania, and access to the PIB database by reporting persons can be done daily.

The security of sending and recording information on payment incidents is ensured by respecting the information regime concerning payment incidents (NBR, 2012a). It is also achieved through banking prohibition, by suspending/resuming/ cancelling entries on payment incidents in the CIP databases, by the organization and management of information on payment incidents recorded in the database of the CIP through the dissemination of the CIP information on payment incidents.

Of course, in addition to our objectives addressed in this paper, the banking information domain is much wider, virtually unlimited, and information security management in this area is a challenge for any researcher interested in this field.

3. The functions of banking information security management

Banking information security management and its functions: planning (providing, forecasting), organization, training (control-motivation), coordination and control manifests itself practically through attributes (functions) of information security, i.e. the characteristics thereof, or the syntactic role that they fulfil, the combination of properties. In literature (Mureşeanu, 2009), we find five attributes (functions) of information security (Fig. 2) which can be grouped as follows:

- Attributes of functionality: the availability of information; confidentiality of information; integrity of information.
- Attributes of injury recovery: authenticity of information; non-repudiation of information.

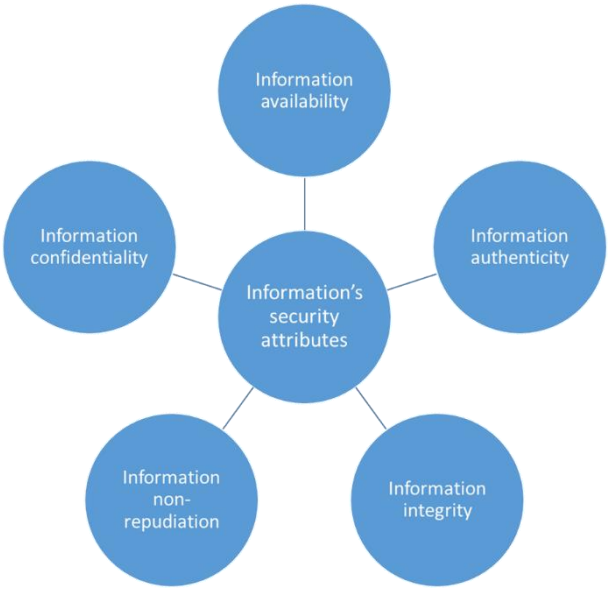

Fig. 2: Information security attributes (Ţigănoaia, 2013)

The availability of banking information is the security attribute and at the same times the element of banking information security management which provides legal users with the information they need. Legal users of the information provided by the Credit Risk Register (CRR) are the reporting persons and the National Bank of Romania (NBR, 2012b), and the users of information concerning the Payment Incidents Bureau (PIB) are the reporting entities, the National Bank of Romania, the Prosecutor's Office of the High Court of Cassation and Justice and the Ministry of Interior, with their territorial units, courts, other state institutions exercising supervision and control and other individuals and legal entities, resident or non-resident, through credit institutions, under the law (NBR, 2012a).

Availability is a crucial aspect related to information, an intrinsic attribute of it, and from this point of view it is the most important function. In general, the more it is used, the more productive and useful information becomes. Information should multiply and become available to users. Specialized studies on the availability of bank information through systems of reporting and management of credit information show that such information can reduce the number of bank failures common to financial markets globally, but especially those of economies in developing countries (Gabriela et al., 2015). Research in the field showed that "the availability of credit information of improved quality is a solution both for solving all types of information asymmetries between debtors and creditors, as well as for issues arising from these, the opponent section and moral hazard reducing the risk of bankruptcy and improving the allocation of credit" (Stiglitz and Weiss, 1981; Pagano and Jappelli, 1993). At the same time the availability of credit information, its dissemination towards market users can promote some responsible 'credit culture', by discouraging excessive leverage, and encourage the "making up" of responsible repayment of the loan (De Javry et al., 2009). We agree thus with the idea that information "produces", creates value as it is used more and more often, and restricting access to information is a hindrance. Of course it is an obligation to ensure availability of public information for all users, according to Law no. 544/2001 on free access to information of public interest, consolidated in 2009.

In the field of banking information, availability is regulated in the databases of the CRR and the PIB, our objectives in this work being regarded as security issues. Thus, given the widespread influence of the intentional factor, it should be treated as a security issue and included in the analysis of security risks itself, "The international factor involves intelligence, it has knowledge and it uses intervention capabilities to achieve its objectives" (Ţigănoaia, 2013); in the case of Credit Risk Register (CRR) information is made available to users through: reporting entities and the National Bank of Romania (NBR, 2012b); by the Central File of Credit (CFC), that is information related to credit risk, reported by the reporting entities, processed and disseminated by the CRR in order to be valued by users under the conditions of professional secrecy; by the Overdue Debt File (ODF) supplied with information by FCC, on a monthly basis, on credit risk at borrowers and their overdue loans to all reporting entities in Romania; available by the File of Groups (FG), powered monthly by FCC with information about groups; available by the File of Card Fraud (FCF) which lists information about fraud with debit and/or credit cards. At the same time, information is available during the cross-border exchange involving CRR, according to the "Memorandum of Understanding on the exchange of information between national credit registers, for their transmission towards reporting entities, entered by the National Bank of Romania with the competent authorities in such matters from the Member States" (NBR, 2012b). Information becomes available at the moment of the transmission and recording of information for credit risk and information about card fraud; it is available on the occasion of organizing and managing credit risk information and information about card fraud, in

accordance to their regime, established by NBR (2012b). The availability of banking information is also regulated by the dissemination of credit risk information and of information about card fraud. The availability of CRR information is ensured in accordance with Appendix 11.2012 of NBR (2012b), and by looking at the information flow diagram of the Central of Credit Risk, as shown in Fig. 3.

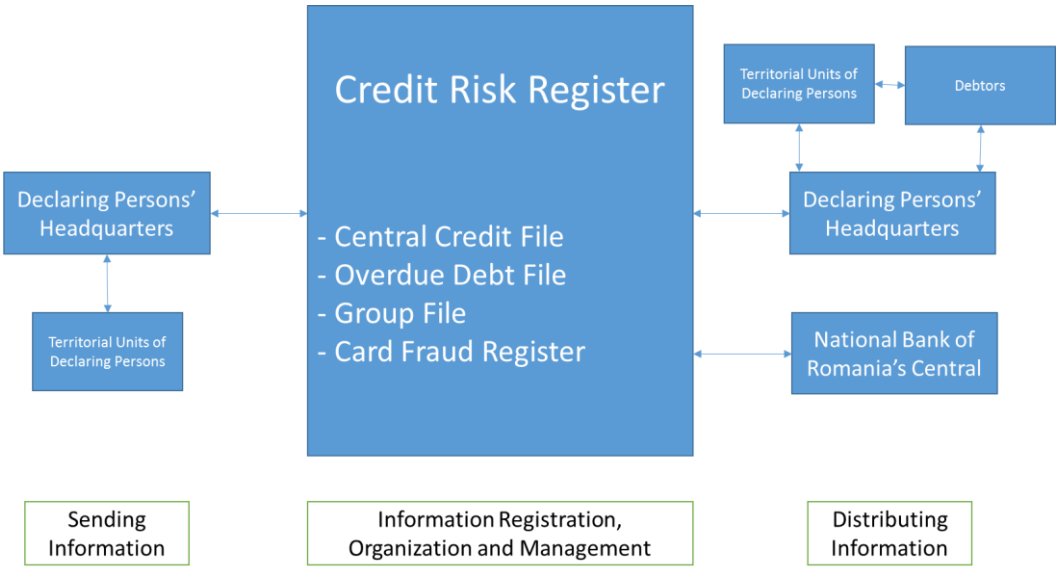

Fig. 3: Availability of banking information by looking at the informational flow of the credit risk register (CRR) (Annex 11 of NBR (2012b) on the organization and functioning of the National Bank of Romania of the Credit Risk Register, Official Gazette, Part I in January 49/20. 2012)

A second approach refers to the availability of information on Payment Incidents in the public interest, including user specific goals, managed by the Payment Incidents Bureau (PIB) of the National Bank of Romania (NBR, 2012a). The availability of such information to their users: reporting persons, NBR, Prosecutor's Office High Court of Cassation and Justice and Ministry of Interior, with their territorial units, courts, other state institutions entrusted with supervision and control; individuals and other legal entities, resident or non-resident, through credit institutions and the law for security by National File of Payment Incidents (NFPI), a file of interest which contains information on payment incidents with checks, bills of exchange, promissory notes structured for each one in particular; National File of Risk Individuals (FNPR), available with information on the major payment incidents registered in the name of an individual or a legal entity, resident or nonresident, powered automatically by FNIP; The availability of such information is ensured with the transmission and recording of information on payment incidents, respecting their regime with the generation of bank ban or the suspension/resuming/canceling of records concerning payment incidents from the CIP database. They are also available at the organization and management of information in databases. All are regulated (NBR, 2012b). Availability of all information held by CIP, concerning payment incidents follows the Information flow of the Payment Incidents Bank (PIB) (Annex 2, 2012 of NBR, 2012a), shown in Fig. 4.

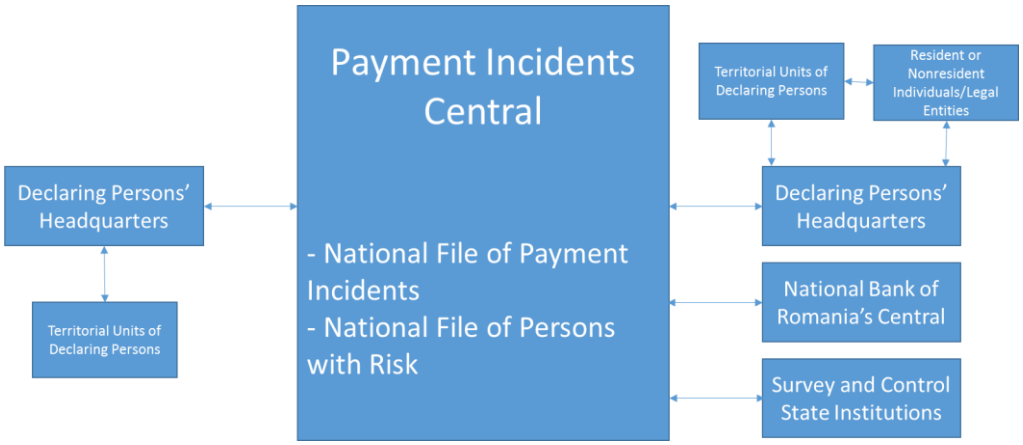

Fig. 4: Availability of banking information following the information flow of the PIB (Annex 2 of NBR (2012a) on the organization and functioning of the National Bank of Romania, the PIB, Official Gazette, Part I in January 49/20. 2012)

Confidentiality of information is a security attribute of functionality. Bank information and banking operations have a confidential character; the actions of transmitting (communication) a secret,

in our case banking information, are also confidential. The confidential character of banking information lies precisely in entrusting their secret. Confidentiality is a prohibition, a limitation, or the blocking of unauthorized/illegitimate users of banking information. It is an exception to the normal use of bank information and therefore it is a consequence of the existence of conflicting interests in society, where the use of information could prejudice certain parties. Protecting the interests of CRC CIP involves defending secrecy and confidentiality.

The means whereby CNC can ensure confidentiality are: managing risk information and information about credit card fraud for the specific purposes of users, in terms of professional secrecy (NBR, 2012b); CRC participates in cross-border exchange of information under the Memorandum of Agreement, on the exchange of information between national credit registers, with the view of transmitting such information towards reporting entities, concluded between the National Bank of Romania and the competent authorities in the matter, in conditions of confidentiality. Credit risk information is the information that is reported, by the reporting entities, and processed and disseminated by CRC, under confidential identification data of borrowers, who may be individuals or legal non-bank entities; it also refers to operations in domestic and foreign currencies whereby the reporting entities are exposed to risk in relation to that borrower; the confidentiality of operations whereby reporting entities are exposed to risk (credit operations, commitments assumed by the reporting person, in the name of the debtor, to an individual, who can be an individual or a legal entity, other than the reporting entities, or to a credit institution / financial institution abroad; the confidentiality of content for assuming commitments, by the reporting person, in the name of the debtor, to another reporting person that operates in Romania; the confidentiality of information about card fraud, information reported, on the fraud or the corresponding amount, by the reporting person as regards contractual provisions, by owners of debit card and/or credit; the confidentiality of individual risk, representing the exposure of a reporting person to a debtor and the determination thereof by the person reporting; the confidentiality of the group of clients who are somehow connected, reported to the CRR by the reporting person; the registering of the reporting person's exposure to at least one of the persons in the group; the confidentiality of the enumerated person (debtor), who may be either a natural or a legal non-bank entity, included in the CRR database as a result of his/her reporting by a declaring person; the confidentiality of global risk, which represents the exposure of all reporting entities in Romania to a single borrower and determined by the CRR. Then, the confidentiality of all information and reporting persons to the CRR, the confidentiality of the entire structure of the database and the access to it. "Credit risk information, sent to or received from the CRR, has a confidential character (NBR, 2012b). When credit risk information or card fraud information is used by trespassing legal regulations, by the reporting persons, these are considered liable, not CRR.

The means whereby the PIB can ensure confidentiality are: the need to protect and manage specific information related to payment incidents, for the public interest, including users' specific aims. The confidentiality of the database organized and managed by the PIB, namely information from the National File of Payment Incidents (NFPI), incidents related to check payments (FNC), incidents related to payment with bank drafts (FNCb), incidents of payment with financial bills (FNBO); information from the National File of Persons with Risk (FNPR), automatically fed by FNIP; the confidentiality of database access by the filling and updating of the "Accreditation form to the PIB of persons authorized to send and receive information about payment incidents; the confidentiality of accessing the informatics system of the PIB and of persons endowed by the PIB with names attributed by the National Bank of Romania; the confidentiality of the daily access to the PIB database by reporting persons.

The following are the means whereby the CRR, as well as the PIB, are able to ensure confidentiality:

- The control of access to information support – informatics support: hardware system, software system, informational flows and circuits by measures of physical protection;
- The control of access to the significance of information/data by encryption
- Information is coded so as to be understood only by authorized persons.

In order to preserve confidentiality, „documents comprising credit risk information or card fraud information, aimed at and received from the CRR, are recorded for 7 years at the reporting persons". NBR (2012a), and information regarding payment incidents, reported to and received from the PIB, are recorded and kept by the reporting persons for 7 years (NBR, 2012a), in accordance to the System Procedure regarding the Control of Documents and the System Procedure for Registering Documents of the Quality Management System, implemented in accordance with the referential requirements and international standards adopted by Romania (SR EN ISO 9000:2006, SR EN 9001:2008, SR EN ISO/CEI 27001:2013).

The integrity of banking information is a security and functionality attribute, aimed at protecting information from either unauthorized or accidental changes. In other words, the protection of banking information is destined to be: cancelled, added, partially or entirely replaced. The integrity of banking information is related to the functioning of banking operations databases and is seen as a security issue. „In the absence of mechanisms for

ensuring the integrity of databases, these accumulate errors and, even if only a small part of such information is affected, the trust in the entire database is lost and the latter should be reconstructed completely" (Țigănoaia, 2013).

In our analysis, in regards to the first objective, we discuss the problem of integrity, and of course of protecting credit risk information and card fraud information for the specific users' purposes, in circumstances that ensure the preservation of professional confidentiality; information from national credit registers participating to the cross-border exchange, with the view of sending such information to reporting persons; the integrity of credit risk information, reported by the declaring persons, which are processed and sent to CRR; the integrity of operations whereby declaring persons are exposed to risk, the integrity of card fraud information reported by the declaring person; the integrity of information concerning individual risk; the integrity of information concerning the enumerated person (debtor); the integrity of information concerning the declaring person; the integrity of information concerning the accredited person; the integrity of information concerning the reporting period; integrity concerning information about users.

Equally important is the integrity of organizing and managing, by the CRR, of the database structure and the access to it, and the integrity of the informational flow concerning the sending, registering, organizing and disseminating credit risk and card fraud information. CRR cannot change credit risk and card fraud information sent by the reporting persons (NBR, 2012b). CRR ensures the integrity of registering information reported by declaring persons and the processing of such information with the aim of obtaining data necessary to users. The integrity of credit risk and card fraud information is maintained in the FRC and the FFC fields for 7 years from the moment of their registration (NBR, 2012b). „The manager of the specialized department of the National Bank of Romania, who coordinates the activity of CRR, can decide upon the ceasing of disseminating credit risk and card fraud information held by CRR, when these have been accessed by unauthorized persons" (NBR, 2012b).

Correcting errors on the information recorded in the database through forms that represent a previous reporting can be done by the declaring person through the use of the form „Notification regarding corrections".

In order to ensure the integrity of information, it can only once go through the conciliation procedure by the census person who contests the correctitude of data included in the CRC database on his/her name, without knowing the reporting person/source of error. The reporting person who gave the information concerning credit risk and card fraud information can be asked to start the conciliation procedure in mostly one working day form the reading of the CRC database.

„Reporting persons are responsible for the accuracy and integrity of credit risk and card fraud information sent to the CRR" (NBR, 2012b).

Among the means of ensuring the integrity of information we can mention (Țigănoaia, 2013):

- "adding a summary to such information", completed with the help of a "parity, CRR, or hash function type, using error detection codes";
- the use of digital signatures

The causing of prejudice can be done through the fraudulent manipulation of information management, characteristic of payment incidents, for the public interest, including for user specific purposes and/or the PIB database structure and the access to it, affecting the integrity of information both through legal provisions or the PIB Regulation (NBR, 2012a). „In general, without specific means, it is difficult to distinguish between an unintentional or accidental change and an intentional one, and it is even more difficult to identify the author and prove the deed" (Țigănoaia, 2013). Among others, one of the functions of banking information security is the „control function", aimed at creating, within the security system, traces and proofs for the instrumentation of such cases.

In regards to the content of the database organized and managed by the PIB, it is crucial to ensure: the integrity of information from The National File of Payment Incidents (NFPI), which includes incidents of payment with check, bankable bills, financial bills; the integrity of information from the National File of Risk Persons (NFRP); the integrity of database access and the filling and updating the form for "Accreditation at the PIB of persons authorized to send and receive information about payment incidents"; the integrity of the name attributed by the National Bank of Romania for the access to the PIB information system; the integrity of daily access to the database by the reporting persons (NBR, 2012a); the integrity of reports to the PIB, by the declaring persons, at the terms and conditions stipulated by regulations (NBR, 2012a); the integrity of information content included in the Informational flow concerning the sending, registering, organization and dissemination of information concerning payment incidents; ensuring the integrity of information content concerning payment incidents of the electronic format that declaring persons send to the PIB through the inter-banking communication network; the integrity of information sent to the PIB by credit institutions concerning the denial of payment of checks, bankable bills and financial bills through the correct and complete filling of the: Form reporting bank refusals with checks, bankable bills and financial bills; "BNR has to ensure, at its headquarters, the technical conditions that would allow the operative and accurate registration, management and dissemination, on electronic support, of information concerning payment incidents" (NBR, 2012a). In order to be included in the PIB database, the information sent by

the declaring person has to meet the content standards and rules of completing forms, stipulated by regulations (NBR, 2012a). The acceptance, by the reporting person, by means of the PIB application, of the "Form for including the bank refusal concerning the check, bankable bill or financial bill" is possible only after the saving of information into the PIB database. "The credit institution must ensure to all customers the forms that include information inscribed in their name, no later than the day following the filing of the refusal at the PIB" (NBR, 2012a). The forms have a regulated content.

Cancelling filed data concerning payment incidents, from the PIB database, can be done by the reporting persons only as a result of a verdict whereby the cancelling is prescribed.

With the aim of obtaining aggregate data needed by users, the PIB ensures the saving of information concerning payment incidents reported by declaring persons and the processing of such information. In order to operatively highlight information concerning: identification of account holders; refusal of checks, bankable bills and financial bills payment, FNIP is managed in accordance with the PIB's own necessities. For the operative character of information evidence concerning: major payment incidents; individuals or legal entities, resident or non-resident, who are denied to write checks, FNRP is managed in accordance with the PIB's own necessities. For integrity purposes, information concerning payment incidents are kept in the PIB databases for a period of 7 years from the moment of their registration (NBR, 2012a), (SR EN ISO 9000:2006, SR EN 9001:2008, SR EN ISO/CEI 27001:2013).

The dissemination of information concerning payment incidents held by the PIB towards users is done in conformity with "The Informational Flow of the Payment Incidents Bureau" (Fig. 2), either by its own decision or at the request of users, in accordance with NBR (2012a). The PIB provides, on request, to the declaring persons, information of payment incidents registered in the database in accordance with the same Regulation. Credit institutions will ensure the customers' right to make out checks where they figure as credit institutions, based on an analysis of risks that involves the respective action. "The manager of the department coordinating the PIB's activity can decide on the cessation of disseminating information concerning payment incidents held by the PIB, when the access to these has been done by unauthorized persons" (NBR, 2012a).

For the accuracy and integrity of information concerning payment incidents sent to the PIB, reporting persons are held responsible. "The PIB updates its own database with the checks authorized by the National Bank of Romania, so as they may be circulated" (NBR, 2012a).

All documents, including information concerning payment incidents reported by and received from the PIB, are saved by reporting persons for a period of 7 years (NBR, 2012a) (SR EN ISO 9000:2006, SR EN 9001:2008, SR EN ISO/CEI 27001:2013).

The authenticity of information is an attribute of prejudice recovery, that attribute of information security that allows the association of information with its author. The author of banking information can be an individual or a legal entity, resident or non-resident, or equipment. "In general, the author of some information is also its generator, or the one introducing the information into the system (Țigănoaia, 2013). The authenticity of banking information credits the accuracy of information, making its producer responsible and giving users the possibility to recover possible prejudices that result from the use of information.

Thus, by managing credit risk and card fraud information for the specific purposes of users, by fulfilling the need for professional confidentiality, it is associated with the Credit Risk Register and the cross-border information exchange, in accordance with the Memorandum of Agreement, associated to the CRC and the competent authorities from Member states, but the information itself are associated to its author (issuing person).

In the analysis concerning the regulation for the organization and functioning, at the National Bank of Romania, of the Payment Incidents Bureau (PIB), for the integrity of information concerning payment incidents, their management is associated with PIB (NBR, 2012a). It can be mentioned here that, as in the management's case, by the CRR, of credit risk and card fraud information, the authenticity by electronic signature of electronic files has a regimen that is equivalent to the holograph signature of the information provider. At the same time, the document including the electronic signature has the same juridical regime as the document certified by private signature.

The following are some general methods for the certification of information:

- Using electronic signatures
- The control of access to information and the activation of a system of log files.

The time stamp can be an indication of the moment of time associated with the electronic document, certified by the authorized signature applied at the moment of signing the document. The time stamp has a juridical value and demonstrates the chronology of some documents (Țigănoaia, 2013). The use of the electronic signature is regulated by:

- Law no 455/201, on the legal regime of electronic systems;
- H.G. no. 1259/2001, concerning technical and methodological norms for the application of Law 455/2011.

The need to prove that some banking information has been forwarded from the sender (reporting person, credit institution, CRR, PIB, BNR, etc.) to the

legal receiver (users, the reporting person, the credit institution, CRR PIB, BNR, etc.), without giving the latter the possibility to contest such an action, in other words the presentation of proofs, traces, non-repudiation proofs, can be developed through the security system. Non-repudiation, as well as integrity, is attributes of the system security, which have to be associated to any banking information, the proof that it has been sent by the sender and subsequently received by the receiver, based on the registered letters principle. The security system can generate such proofs at the moment of editing the document that includes banking information or at the moment of electronically sending it, using the electronic signature of both the sender and of the receiver.

4. Mechanisms that ensure the security of banking information

Information security is ensured with the help of certain mechanisms, among which: cryptographic, biometric and steganographic mechanisms. These can be used for ensuring the security of banking information, along the „applications of such mechanisms, for instance the biometric passport, a new steganographic system forms secure communications, designed and implemented by the author" (Țigănoaia, 2013).

We emphasize here that the cryptographic mechanism is employed for ensuring the security of banking information. Cryptography refers to the application of some banking data codification rules and ensures a safe protection of communication between two entities: reporting person – CRR; CRR – reporting person; reporting person – BNR; BNR – reporting person; reporting person – PIB; PIB – reporting person, etc. The method is based on numerous codification/data encryption techniques. Encryption can be achieved by using either secret keys or public keys.

Of course, the development in the field of computing has triggered a similar development of encryption principles from algorithms with secret keys, however, these are based on traditional methods such as transposition or substitution. „Algorithms with secret keys are characterized by the fact that they use the same key both for the encryption and for the decrypting process. These are called symmetric algorithms. The key has to be well preserved and needs to be known only by the sender on the one hand and the receiver on the other hand" (Țigănoaia, 2013). The main disadvantage of algorithms with symmetrical keys is that they need a security channel between sender and receiver „ for the transmission of the key before the actual encryption process starts" (Țigănoaia, 2013). The encryption process with symmetrical keys, adapted and presented in" (Țigănoaia, 2013), appears in Fig. 5.

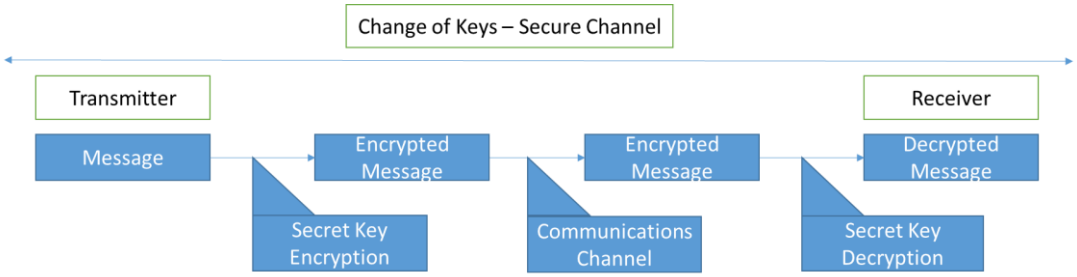

Fig. 5: Symmetrical keys encryption (Țigănoaia, 2013)

In our analysis concerning the security of credit risk and card fraud information, for the specific purposes of users, in conditions of keeping the professional secret, the algorithms with secret key use the same key both in the encryption process and in the decrypting one, therefore they are symmetrical. The key has to be well-known by the declaring persons, their territorial units, the Credit Risk Register, the enumerated persons (debtor), the BNR Register, as sender – the encryption key, but also by the receiver – the decrypting key. The CRR information flow is presented in Fig. 6.

As shown in the figure above, it can be noticed that, from the HEADQUARTERS OF THE REPORTING PERSONS (established by regulations and laws referred to in the previous chapters), information is sent with the help of secret encrypting keys, both of the central and of TERRITORIAL UNITS OF REPORTING PERSONS through security channels, towards the CREDIT RISK REGISTER (The Central file of Credits, the File of Overdue Loans, the File of Groups, the File of Card Frauds), and these decrypt the message, using the same keys. The encrypting key is sent by the CRR before the beginning of the encrypting process through a channel made secure by the declaring person, and this sends it further towards its territorial units. At the same time, by the same procedure, encrypted information is sent from the REGISTER OF THE NATIONAL BANK OF ROMANIA to the CRR and the REPORTING PERSONS, and through these to their TERRITORIA UNITS AND ENUMERATED PERSONS (DEBTORS). The encrypting or decrypting keys are sent by the CRR before the beginning of the encrypting/decrypting process, through a secure channel to: BNR, reporting persons, territorial units and enumerated persons.

In a reversed order, THE CREDIT RISK REGISTER sends information with the help of secret encrypted keys to REPORTING PPERSONS and through these to THE TERRITORIAL UNITS OF REPORTING PERSONS

or TO THE ENUMERATED PERSONS (DEBTORS), as well as to the NATIONAL BANK OF ROMANIA. Adopting the encrypting principle from secret key algorithms, CRR sends the encrypting/decrypting key before the beginning of the decrypting process, through a security channel.

Fig. 6: Asymmetric (secret) key encrypting of information, on the informational flow of the credit risk register (CRR) (Țigănoaia, 2013; NBR, 2012b)

Evaluating the necessity of security for information specific to payment incidents, for the public interest, including for users' specific purposes, in the conditions of preserving the professional secret, the secret key algorithms use the same key in the encrypting and the decrypting processes, thus they are symmetrical. The key has to be known very well by the declaring persons, their territorial units, the Payment Incidents Bureau, BNR, state institutions with attributions of supervision and control, but also as receiver of these – the decrypting key. In this context we put forward the structure in Fig. 7, which concerns the Information Flow of CRR. Fig. 7 shows that THE HEADQUARTERS OF THE REPORTING PERSONS (established by laws and regulations and presented in previous chapters) encrypted information is sent with the help of secret encrypted keys, belonging to the TERRITORIAL UNITS OF REPORTING PERSONS, through security channels, towards THE PAYMENT INCIDENTS BUREAU (The National File of Payment Incidents; The National File of Risk Persons), where the message is decrypted, using the same keys. The same procedure applies to the sending of encrypted information from the REGISTER OF THE NATIONAL BANK OF ROMANIA towards PIB and REPORTING PERSONS, through these, to their TERRITORIAL UNITS, as well to individuals or legal entities, either resident or non-resident, towards state institutions with attributions of supervision and control. The encrypting or the decrypting key is sent by PIB before the beginning of the encrypting/decrypting process, through a security channel to: BNR, reporting persons, the territorial units of the latter and the enumerated persons, and also to state institutions with attributes of supervision and control.

In reversed order, THE PAYMENT INCIDENTS BUREAU sends information encrypted with the help of the secret encrypting keys to the REPORTING PERSONS and through them to THE TERRITORIAL UNITS OF REPORING PERSONS or the INDIVIDUALS OR LEGAL ENTITIES, RESIDENT OR NON-RESIDENT, STATE INSTITUTIOS WITH ATTRIBUTIONS OF SUPERVISION AND CONTROL, as well as to the NATIONAL BANK OF ROMANIA. In accordance with the principle of encrypting with secret keys algorithms, the CRR sends the encrypting/decrypting key before the beginning of the decrypting process, through a security channel.

If we approach the encrypting with (public) asymmetric keys, we have to understand that „ encrypting algorithms using public keys are characterized by the fact that the encrypting process does not use the same key employed in the decrypting process" (Țigănoaia, 2013). Thus, in such a situation, the algorithms are called asymmetrical keys algorithms. The situation requires the distribution to anyone of the public key, while the private key remains secret.

Another mechanism is the biometric one, which emphasizes the applicability of signature on credit risk information and on information about card frauds, in the case of the CRR, on information specific to payment incidents, as a form of access administration and control. According to laws (Law no. 455/2001), "the electronic signature represents a collection of data incorporated in electronic format,

attached to or associated to some electronic format piece of writing, with the intention of producing legal effects that would allow the formal identification of the signing person. The electronic signature represents a digital form of the holograph signature, having the same functionality and applicability as the holograph signature. It presents the advantage of offering a high degree of security as regards the integrity of data and ensuring non-repudiation – there are no suspicions in regards to the identity of the person signing the document. In fact, electronic signature appears in the form of data attached to credit risk information, card fraud information but also payment incidents information, in order to ensure security. "Digital signature is a sequence of data in electronic format, obtained by the asymmetric encrypting logic associated to an entity (message, document, file), also in electronic form, which ensures the support for services of identifying the origin of the entity it is attached to (authentication), checking the integrity of content and the subsequent non-repudiation by the signing person of the signed entity" (Neagu, 2009). The public key encrypting system is used for digital signatures, thus a digital certificate, provided by an authority (BNR), is required.

Technically speaking, as indicated by specialists (Ţigănoaia, 2013), the devices for creating digital signatures are either software applications, or hardware devices that are properly configured. A device for creating digital signatures "must have the following properties: it should not allow the deduction of data on which the digital signature is created; it should change no data that must be signed; it should have mechanisms for ensuring the confidentiality of data used for creating the digital signature (Ţigănoaia, 2013).

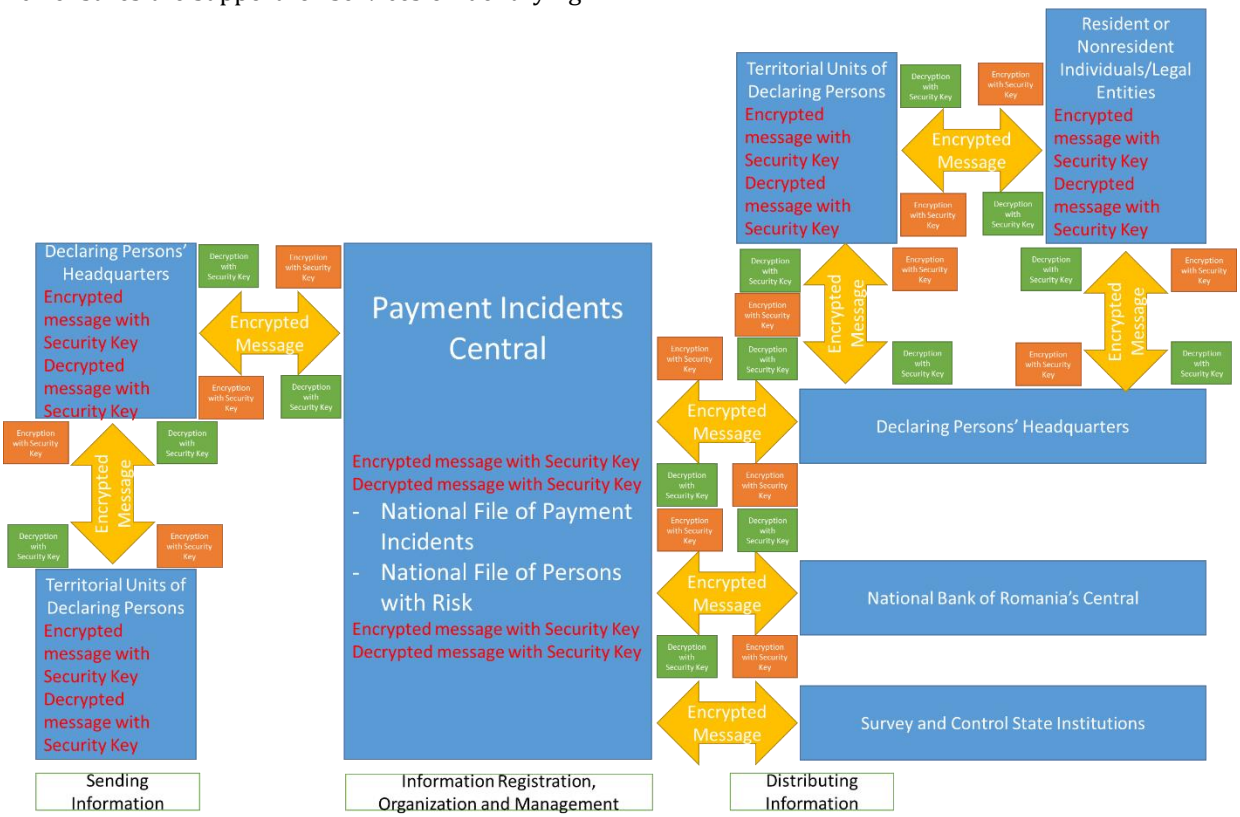

Fig. 7: Secret key encryption of the information flow of the payment incidents berau (Ţigănoaia, 2013; NBR, 2012a)

5. Conclusion

With the view of diminishing credit risk, both at micro-prudential level, from the perspective of credit and non-banking financial institutions, and at the macro-prudential level, from the perspective of strengthening supervision and regulations, and with the view of preserving financial stability in Romania, the functions and roles of the place held by the public credit register in Romania and especially the type of information it receives, organizes and manages or disseminates, have to be well understood. The Credit Risk Register is a modern and flexible system of report and administration of credit-related information in Romania, relying on principles and a strong architecture of data base, with credit information flows and credit information whose dissemination and use are clearly set. The architecture of this central credit register uses an efficient informatics system, used for achieving the harmonization of credit information, from the community level to the other participants in processes of data gathering, and risk information from central banks of the European Union.

The research concerning the efficiency and the consolidation degree of the non-payment risk management system, generated by the use of debit payment instruments in Romania is relevant for the management of banking information security. The National Bank of Romania tries to understand the payment behavior of account holders by looking at payment incidents reported by credit institutions at

the Payment Incidents Bureau, in accordance with current regulations. The activity of the PIB ensures the presence of a centralized and updated source of information concerning payment refusals of debit instruments and contributes to the increase of awareness concerning legal provisions and regulations concerning debit payment instruments and security of their use. At the same time, it is a security partner for credit institutions in the process of preventing, evaluating and limiting risks associated with unreliable customers.

Both the CRR and the PIB have profound implications in the banking domain and implicitly in real economy, providing correct and detailed information, offering support in making decisions regarding the prevention and fighting against credit risk or non-payment risk, contributing by the early warning on system risks and ensuring financial stability.

The content of management, especially the process whereby information is transposed into action by means of decisions, is largely determined by the information system, on which decision-making relies (Rada et al., 2014).

We have seen that, in all fields of human activity, information is an active and crucial participant to the development process and to progress; it also contributes to reducing risk and uncertainty (the Balck Swans) (Taleb, 2010; 2014; Constantin and Doina, 2016; Doina and Constantin, 2016), and to a reliable scientific proof of specific policies and strategies.

References

Argyris C (1992). Dictionary of information sciences and technology. Academic Press, Boston, USA.

Benyon D (1990) Information and Data Modelling. Blackwell Scientific Publications, Oxford, UK.

Clifton HD (1990). Business data systems: a practical guide to systems analysis and data processing. Prentice Hall International (UK) Ltd., London, UK.

Constantin RI and Doina ML (2016). Forms of communication and strategies adopted by managers and economists engineers in the "BLACK SWAN" situation of social economy. International Journal of Modern Communication Technologies and Research, 4(2), 19-22.

De Javry A, Mcintosh C Sadoulet E (2009). The supply- and demand-side impacts of credit market information. Journal of Development Economics, 93(2): 173-188.

Doina ML and Constantin RI (2016). The antifragile of decisions adopted by managers and engineers economists working in the sector of vulnerable groups' social economy. International Journal of Modern Communication Technologies & Research (IJMCTR), 4(3). Available online at: https://www.erpublication.org/admin/vol_issue2/upload%20Image/IJMCTR041301.pdf

Gabriela T, Georgiana G, Alina S, Mariana P, and Gabriela Z (2015). Caiete de studii Nr. 40: Experienţe internaţionale privind utilizarea bazelor de date referitoare la Centrala Riscului de Credit şi la Centrala Incidentelor de Plăţi. Banca Naţională a României [National Bank of Romania], Bucureşti, Romania.

Lucey T (1991). Management information systems, DP Publication Limited, London, UK.

Mureşeanu G (2009). Settlements regarding the actities of CERT structures, Ph.D. Dissertation.

NBR (2012a). Regulament nr.1 privind organizarea şi funcţionarea la Banca Naţională a României a Centralei Incidentelor de Plăţi. National Bank of Romania [Banca Naţională a României], Publicat în Monitorul Oficial, Partea I 49 la 20 ian.2012, Bucureşti, Romania.

NBR (2012b). Regulament nr.2 privind organizarea şi funcţionarea la Banca Naţională a României a Centralei Riscului de Credit. National Bank of Romania [Banca Naţională a României], Publicat în Monitorul Oficial, Partea I 49 la 20 ian.2012, Bucureşti, Romania.

Neagu G (2009). Politica şi arhitectura securităţii datelor în Internet. Note de curs, Program de master, Universitatea Politehnică, Bucureşti, Romania.

Pagano M and Jappelli T (1993). Information sharing in credit markets. The Journal of Finance, 48(5): 1693-1718.

Rada IC, Rada Ioana C, Ursu AR, and Kövendi Z (2014). Management. Universităţii din Oradea, Oradea, Romania.

Stiglitz JE and Weiss A (1981). Credit rationing in markets with imperfect information. The American Economic Review, 71(3): 393-410.

Taleb NN (2010). The black swan: the impact of the highly improbable [Lebăda neagră: impactul foarte puţin probabilului]. Curtea Veche Publishing, Bucureşti, Romania.

Taleb NN (2014). Antifragile: Things that gain from disorder [Antifragil: ce avem de câştigat de pe urma dezordinii]. Curtea Veche Publishing, Bucureşti, Romania.

Ţigănoaia B (2013). Asigurarea securităţii informaţiilor în organizaţii. apărută în seria Studii strategice şi de securitate la Editura Institutul European. Available online at: www.euroinst.ro

Watters C (1992). Dictionary of information sciences and technology. Academic Press, Cambridge, USA.