Mihai MIEILĂ (1)
Valahia University of Târgoviște
Corneliu Vișoianu (2)
Valahia University of Târgoviște
Cezar OSICEANU (3)
Valahia University of Târgoviște

SECURITY INFORMATION AND SECURITY GUARANTEES OF INFORMATION PROVIDED IN A REENGINEERING PROCESS

Abstract:	*Following the analysis of the theories specific to the process of carrying out a Business Reengineering Plan (BPR), from the perspective of the security of the information provided and the security guarantees offered to the management of any such process, we consider that a systemic approach to introduce the subject among the central themes of the term is needed.* *Management reengineering and/or management reengineering at the organizational/corporate level is one of the major challenges facing the shareholders/owners of a company that initiates such an approach today.* *The lack of information protection and the guarantee of its security, within the concept of reengineering, especially in the current society conditions (characterized by major economic effects caused by crises, pandemics, cyber attacks, etc.), is one of the big unresolved problems of reengineering but also the major reason for the distrust of employees in companies subject to this process.* *As a solution, we propose the introduction in the Reengineering Plan of a new step, called security, along with the seven steps of classic reengineering, in view of the need to ensure information security during the process, a step that thus becomes conditional.* *At the same time, the stability of the BPR is characterized by a state of resilience, based on the balance of three components: organizational culture/trust, team professionalism and technological level appropriate to the legal environments, which only in reciprocal balance can ensure the success of the process.*
Keywords:	**Reengineering; information management; information society; Business Plan of Reengineering – BPR; information security; security guarantees; information resilience**
Contact details of the authors:	E-mail: mihai.mieila@yahoo.com (1) corneliu@visoianu.ro (2) cezarosiceanu@yahoo.com (3)

Institutional affiliation of the authors:	**Valahia University of Targoviste**
Institutions address:	Lt.Stancu Ion street, No. 35 – 130105, Târgovişte, România; Tel/Fax: +40-245-206104, http://scoaladoctorala.valahia.ro/

Introduction

The need to analyze this aspect related to information security and security guarantees offered in a reengineering process, an aspect not highlighted at all so far in any paper published on this topic, also takes into account the two currents of presentation of doctoral theses on this topic. . In fact, it is the *"classicist"* and *"synonymous"* current of these works recorded and published on the subject of reengineering. Basically, the "classicists" take over what was written and stated before them by the coryphaeus of the term, and the "synonymists" - majority in number, prefer to use synonyms commonly in defining the same terms and their analyzes as in the works of their predecessors.

That is why the very existence of these two currents may have caused the above-mentioned issue to be overlooked, although its importance is major in the case of a Business Reengineering Plan/Business Plan of Reengineering (hereinafter referred to as BPR). Another reason for not analyzing this aspect is that the vast majority of those who wrote on this topic of reengineering were trained by economists and this issue falls very much to the information analysts and specialized lawyers.

The method used so far to ensure that this aspect consisted only of simple contractual clauses of confidentiality extremely difficult to implement in practice, due to legal issues such as deadlines, legal proceedings, legislative inconsistencies between states, cumulated and with the high degree of failure of reengineering processes, procedural fees etc.

In a major challenge, from the evolution of the current society to the fulfillment of the criteria established for an information society, the protection of information and security guarantees become vital to any business or BPR.

Literature review

Michael Hammer and James A. Champy[1] are considered to be the parents of reengineering itself, they are the ones who defined and launched the concept and Bhudeb Chakravarti[2] is the one who will later launch the "seven steps theory of reengineering"called by us: INSPIRE by using the initials of these steps. Adam

[1] Michael Hammer, James Champy, *Reengineering the Corporation: A Manifesto for Business Revolution*, Harper Collins Publisher, New York, 2006

[2] Bhudeb Chakravarti, *Business process management*, https://www.bhudeb.com/bpm-bpr#inbox/_blank, (16.04.2022)

Smith[1] said in 1776 that "the division of labor is the essence of industrialization and the progress of mankind" while Frederick Winslow Taylor- the founder of scientific management, propagated Adam Smith's principle of the social division of labor as a guarantee of the success of any human activity. At the same time, however, the procedural approach in management, first proposed by Henry Fayol[23], represents the management process in terms of the five functions of management, Fayol linking the evolution of the procedural approach to increasing the importance of mutual relations. In our opinion as a complement to this concept stated by Hammer and Champy, the following three principles appeared in 1994, principles that senior management should know before starting a BPR Bussiness Process of Reengineering).

1. Changing a management process focuses on external objectives, because all those objectives that may involve the outcome of the process in customer satisfaction;
2. Coordination of complex horizontal activities will require first of all the development of connections and boundaries in the same plane;
3. Management team members should have primary access to all unfiltered information in a way that is easy for them to access. Al Mashari and Zairi[4] in particular, rightly insist that the relocation and resizing of the IT network are major factors in the success of the BPR implementation process. Viewed from the perspective of Koestler's Holonic theory[5], the internal capacity of the company offered by the internal Intranet system, ensures a true holistic business system structure.

The term BPR differs substantially from common practice and can be a "process innovation" according to Thomas Davenport[6] while Attaran and Wood[7] they claim that: "the ultimate theme of a business process is to find the means to improve which in turn will generate rapid and substantial gains for the company's

[1] Adam Smith, *The Wealth of Nations*, Chapter I - Of the division of labor, Wordworth, Stansted, 1776

[2] Frederick Winslow Taylor, *The Principles of Scientific Management*, Dover Publications, Mineola, New York, p. 43

[3] Henry Fayol, (1949), *General and Industrial Management*, Dover Publication, Mineola New York, 1911, p 43

[4] Majed Al-Mashari,Mohamed Zairi, *Revisiting BPR: a Holistic Review of Practice and Development,* ”Business Process Management Journal”, March 2000, https://www.emerald.com/insight/content/doi/10.1108/14637150010283045/full/html, (16.05.2022)

[5] Arthur Koestler, *The Ghost in the Machine* , Hutchinson, London, 1967

[6] Thomas H. Davenport, J. Gilbert, B. Probst Heinrich von Pierer, *Knowledge Management Case Book*, , 2nd Edition, Siemens Best Practice, 2002, p. 10

[7] Mohsen Attaran, Glenn Wood, *How to Succeed at Reengineering*, ”Journal of Management Decision”, vol. 37, No. 10/1999, p. 37

performance". To understand the importance of information management we must mention the following[1]:

1. Any information system in a business must comprise all the data, information, procedures, information circuits and methods used in the information process, which presupposes the existence of a complex, and as secure as possible, a mechanism for collecting, processing, storage, use and transmission of data and information.
2. The general components of an information system are: data and information, information circuit, information procedure and means of information processing, data protection means, mechanisms for guaranteeing data and information protection.
3. The data stored or not, in circulation or in storage, are represented by facts, processes, situations, mechanisms, events expressed lyrically or numerically, being the symbolic support of the information of a business. All this data is organized and recorded in turn in a complex set of data that gives their operator the exact way to know about the organization, resources, results and its environment.
4. Criteria for the existence, sorting, presentation, communication and use of information recorded in an organizational system:

a) By mode of communication: oral information; written information; audio-visual information;

b) By character: information free to be known, information with internal degree of security, sensitive information;

c) By origin and destination: internal information, external information, official information, unofficial information;

d) By direction of travel: ascending information, descending information, collateral information;

e) According to their importance for the organization: secret information with limited use of top management, restricted circuit information, public information;

f) According to the level of legal protection: information protected by the laws on intellectual property protection for which the specific procedures were performed by the organization officials, information protected by the laws on intellectual property protection for which the specific procedures were not performed by the organization officials, information and programs guaranteed in terms of their security.

Accurate, correctly selected, and quality information is critical to creating an effective information system within a BPR without which the team in charge of building the proposed model cannot achieve the purpose for which it was requested. That is why there are common procedures for defining terms related to the information system, information protection and guaranteeing information

[1] M. Petrescu, A.G. Petrescu, Fl. R. Bilcan, V.A.Camarasan, *Tools and mechanisms regarding the management of classified information – From theory to practice,* Biblioteca Targoviste, Târgoviște, 2019

regardless of the field of activity, as they are generally applicable. Any reengineering activity will be analyzed in the following "seven steps" [1]:

1. *Information circuits,* ie itineraries of data, information and decisions from the issuer to the beneficiary.

2. *The information procedure* or the set of elements for establishing and using the methods of collecting, processing and transmitting the information contained in certain *information circuits.* The procedures in question are based on certain instructions, models and algorithms through which the data become information, while acquiring a high degree of formalization and typing based on which their sorting, securing, application and guarantee are done.

3. *The means of processing* information which are in fact all the methods of collecting, storing, recording, processing and transmitting data and information may be: normal, mechanical and/or computerized.

4. *How to collect, process and disseminate information within the organization.* Gathering information is, from a theoretical point of view, a complex process of researching formal and informal sources, practical conditions of access and technical devices necessary for gathering and most information leaks outside the organization are based on systemic problems. to these.

5. *Determining the strategic priorities and the elements of impact on its activity is part of the analysis process within an BPR.* Specifically, the reengineering team must identify the information available to it for decision-making in appropriate conditions. Depending on these, as well as on the team's own, it will be possible to proceed to the formation of the informal plan on the model proposed to the organization.

6. *Information plan.* The result of the analysis must necessarily identify, concretize and visualize the differences between the current sources of information (of the organization and the reengineering team) as well as the priority areas of research. This plan is the product of the strategic and operational queries of the organization made by the reengineering team and indicates the real level of financial, human and informational resources of the organization as well as its development and maturity.

7. *Establishing the priority areas of the analysis within a BPR in terms of information* includes the following actions[2]

- Identifying people and means of internal research
- Verification of internal and external sources of information and research
- Creating an effective filter for the intended purpose in order to select only the necessary information
- Classification of information and sources
- Creating a scale based on the urgency of the need for information and the importance of information
- Determining exactly the beneficiaries of the information

[1] *Idem*

[2] *Idem*

- Communicating the tasks related to this subject to the personnel with attributions in the field within the organization subject to reengineering.

Normally any organization should be able to make unrestricted use of the means and methods of gathering legal information, and by using directly or indirectly accessible sources of information, it will usually be able to obtain sufficient data and information. Therefore, the organization itself must know very well the information it holds and disposes of, so as not to end up in the situation of looking for information it already has (the most common case is related to the possession and validity of copyright, patents, inventions, etc.). Thus, if the information plan, developed by the reengineering team based on the information provided by the heads of the organization subject to reengineering, is properly implemented, it will become the basis for building the model proposed by BPR for approval to top management or shareholders. The first problems that arise are in this area, because the organization undergoing reengineering does not provide all the real and necessary data - from the desire to protect itself but also from the lack of guarantees offered by the team performing the reengineering. Because of this, in the model proposed by the team, the first distortions begin to appear , smaller or larger but important enough to alter the success of such an activity.

On the other hand, the organization intentionally underestimates the availability of much of the necessary information, based on the idea that it would fall into the category of confidential information.

In order to obtain the necessary data and then to carry out a correct analysis of the organization , the members of the engineering team must:

- have the ability to understand development priority;
- have technical knowledge to enable them to understand the meaning of the information gathered;
- possess data and knowledge regarding the organizational culture of the analyzed business - use a common language of communication, preferably that of the majority nationality within the analyzed organization;
- to present certain security guarantees to the organization and to the employer.

It should be noted that almost half of the information sought outside an organization is actually found inside it, which is determined by the fact that the information available to the organization is not correct and properly structured and therefore any information that has become publicly accessible. During the work of the reengineering team, it will arouse suspicions of unauthorized leaks and the first to be targeted will be the members of the reengineering team.

Guarantees of information security in a reengineering process

In order to be able to request guarantees of information security in a reengineering process, we must start from some important and obligatory premises as follows:

1. Defining the concept of information: information can be presented and constituted in many ways and from different perspectives, in general, however, it is

represented by documents, data, objects or activities, regardless of their medium, form, mode of expression or circulation.

2. Knowing the classifications of information from a legal point of view

According to the legislation approved, published and in force in Romania, the information is classified as follows:[1]

- Non-advertising information[2] ;
- Information of public interest[3];
- Unclassified information;
- Personal data information[4];
- Classified information[5] .

3. "Nemo censetur ignorare legem - Ignorance of the law does not absolve from the guilt of its non-observance!"[6]. Knowledge of the legal principle valid in any national system stated in the title by any member of a reengineering team is mandatory because "No one is above the law!"[7].

Also, the knowledge and observance of the related laws at local, regional, national, continental, global and sectoral level is strictly obligatory for the members of the reengineering teams because their violations are the reasons for the need for reengineering or the reasons for the failure of reengineering. It is well known that many companies have sensitive data, secret service data, classified data, patents and inventions, impact contracts, etc. and access to them is strictly restricted[8].

As we mentioned before, access to this data is not desired by the shareholders of the company undergoing reengineering given the effects of their knowledge outside the company. Access to this data by a team outside the company, even if its role is obviously objective and sustainable, has highlighted a possible "Trojan horse" of reengineering. We must take into account the situation that existed after the 1990^s, when the military-geopolitical blocs disappeared, the Eastern society was preparing to adapt to the demands of the typical consumption of the West, the West wanted the secrets of the East. the two great currents (American and European), the rapid spread of the computerization of society, etc. The question that arises regarding this sensitive area of the guarantees offered by reengineering teams and the non-inclusion of this aspect in the circle of graphic

[1] *Idem*

[2] Petre , Burlan Daniel, *The New Criminal Code* , Rosetti International, București, 2020, art. 304

[3] *Law 544/12.10.2001 Regarding the free access to information of public interest* , Monitorul Oficial no. 663 /23.10.2001

[4] https://gdpr.eu/ Complete Guide to GDPR compliance, (18.02.2022)

[5] *Law 182/12.01.202 Regarding the protection of classified information,* Monitorul Oficial No. 248/12.04.2002

[6]Romanian Constitution,, art . 1

[7]Romanian Constitution, art. 16, paragraph 2

[8] M. Petrescu, A.G. Petrescu, Fl. R. Bilcan, V.A.Camarasan, *Op.cit,* p. 20

representations of reengineering is the following: "Why aren't security guarantees offered in a reengineering process?". Here are some possible answers from the theory and practice of reengineering:

1. The process of reengineering from a theoretical point of view does not provide anything about compliance with information security and ensuring their security by the team hired to perform this activity.

2. Reengineering, created after 1990, was indirectly aimed at finding out information inside the organization, secret information, internal circulation, etc. so that it could be used unofficially later! This is how the Israeli intelligence systems managed to get the technical documentation of both the parts of the Soviet-made MIG 21 fighter jets and the tools, systems, etc. that produced the tools, subassemblies and parts. As a result of a reengineering offered to repair companies outside Russia, accredited for this aircraft, this was possible, which allowed Israel to gain control of the international military arms market, an extremely popular product and present in military aviation. of most states in the sphere of ex-Soviet influence, many of these states having enemy status,

3. Negotiations establishing the contractual terms of such a process should have included both the "winning premium" and the "interest insurance" in case of failure, information leakage, etc. As payments are made in part in advance, in theory a special fund should be set up which would increase costs and lead to the immobilization of significant financial funds, in addition to long-term legal actions, high costs, additional staffing and resources, and an unforeseen end.

Author's theory of the seven steps of reengineering through the prism of information security in a bpr

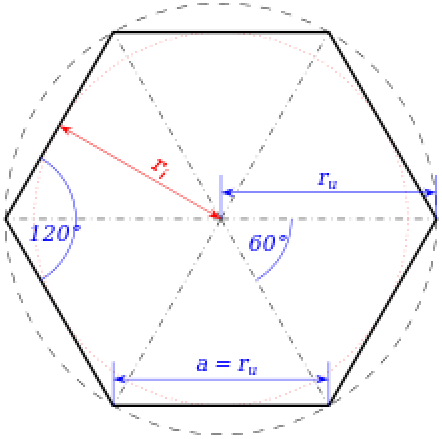

Fig 1. The geometrical figure of a regular hexagon
Source: Authors

The regular hexagon is a regular convex polygon with six equal sides. Its internal angles are congruent, each measuring 120° (the sum of the measures of its angles being 720°, as in any hexagon). The circle around a regular hexagon has a radius equal to the side of that hexagon. The circle inscribed in a regular hexagon has a radius equal to $L_6 \sqrt{3}/2$, where L_6 is the side of that hexagon. In plane geometry, the apothem ri of a regular polygon is one of the right segments that connect the center of the polygon with the middle of one of the sides (figure above), but this term can also refer to the length of this segment. Until now, any economic analyst who is involved in creating a BPR had to follow the "seven steps of reengineering" (INSPIRE in English and INSPIRA in Romanian) ordered as such by Bhudeb Chakravarti and considered axiomatic in the whole thinking of management, because they are the very stages of the process:

1. Initiating the reengineering process and preparing the *"business case"*;
2. Negotiating with the senior business management and approving the start of the construction of the BPR project;
3. Selecting key areas where reengineering is needed;
4. Planning the reengineering process and its stages;
5. Investigating the causes and analyzing the reasons why the problems appeared in the areas discovered to be weak;
6. Redesign (redesign) of areas discovered to have problems in order to increase performance;
7. Ensuring the successful implementation of the plan through continuous monitoring and evaluation. In our opinion, steps 1 and 2 are obviously so closely linked that they can easily be merged with what we have called information protection and security guarantees; security in a reengineering process is practically one of the mandatory steps of the process called security.

We suggest that for the visualization of a BPR of any type, the formula of a regular hexagon inscribed in a circle, starting from the idea that an equilateral triangle represents the best and really one of the segments of any such plan. Until now, the idea induced by the shape of the pyramid has been frequently used to explain the processes and organization charts of a business, company etc. Although the graphic representations in all published works indicate a triangle called "pyramid". In this way we will have 6 equilateral triangles that represent these steps numbered as follows:

1. Initiation of the reengineering process, preparation of the "business case" and negotiation with senior business management and approval of the start of construction of the BPR project
2. Selection of areas key where it is necessary to intervene by reengineering
3. Planning the reengineering process and its stages
4. Investigate the causes and analyze the reasons why the problems appeared in the areas discovered to be weak
5. Redesign (redesign) of areas discovered to have problems in order to increase performance.
6. Ensuring the successful implementation of the plan through continuous monitoring and evaluation.

In order to ensure the balance and to maintain the unity of the regular shape of the hexagon, in fact of a BPR, each triangle must keep its qualities and properties of an equilateral triangle. This is due to the equality and importance of each step in a BPR. The demarcation areas between the steps are represented by the radii of the circle and thus ensure that at least two sides of the triangle are permanently equal. The natural tendency is for each step - triangle, to tend to increase at the expense of the other steps - the other triangles. In order to maintain a control that ensures the maintenance of the evenness of the step itself, it is acted with a calculable force using the apothem which is also theoretically equal for any of the six equilateral triangles of the BPR[1]. In other words, for the leader of a BPR, theoretically the same force should be needed to maintain the implementation of such a process. This means streamlining the management process of the management of a BPR and reducing the consumption of resources involved in the BPR process. The apex of the hexagon is also the force that maintains the evenness of the triangle but also the communication channel with each internal segment of the triangle from top to bottom and from bottom to top. Because the sphere is the perfect shape in geometry in space and the circle is the perfect shape in plane geometry. Therefore, for a BPR to be perfect, it is necessary to present it in the form of a circle, as most researchers do.

At this point, however, we will find that the spaces outside the regular hexagon represented by the BPR plan itself are also six in number, the areas of which can also be calculated. Basically, these six areas are the ones that constitute step 7 = security, though the one of information protection and security guarantees in a BPR, they are also the protection and buffer zones against disturbing actions both inside and outside. The two points of contact of each triangle with the edge of the circle circumscribed by the hexagon represent the minimum average of the possibilities of disturbing the balance of the information protection system and of the security guarantees, though of trying to penetrate from the outside or leaking information from the inside.

[1] *Property 2. In an equilateral triangle, all the important lines starting from the same vertex coincide (the bisectors of the angles coincide with the heights, medians and mediators). These are also axes of symmetry.* https://liceunet.ro/ghid-geometrie/coliniaritate-concurenta-paralelism/centrul-cercului-circumscris-relatia-lui-sylvester, (18.02.2022)

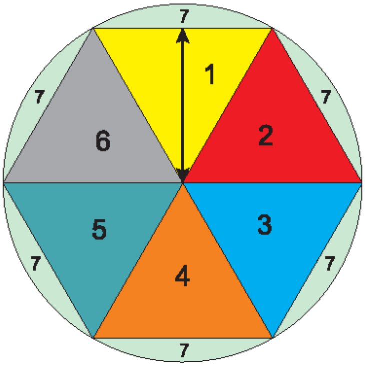

Fig. 2 Case studies in the analysis of the information protection system within the Osiceanu Theory model
Source: Author

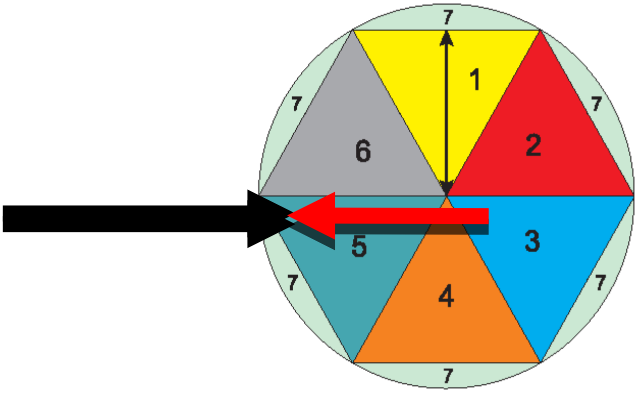

Fig. 3 Scenario 1: Attack on the system executed from outside of it
Source: Author

FE = External force is :
- a disruptive external force of the system which consists of actions of the market, of competition, of certain persons or groups, as a result of changes in legislation or the environment, etc.

FR = Inner force is a force :
- response, internal to the system
- designed and constructed with the construction of the system itself to ensure the balance of the system in relation to the external disturbing force that may occur
- equal in any point of contact with the outside being represented from a mathematical point of view by the radius of the circle

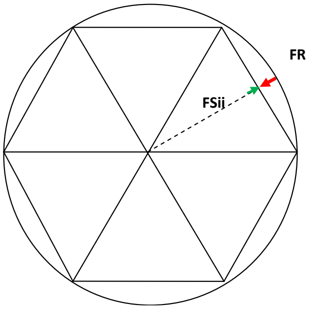

Fig. 4. Scenario 2: Leakage of information inside the system
Source: Author

FSII - The force of information leaks inside the system:
- is generally low in value due to the small number of employees who may try to either test the reaction force of the system or even try to penetrate security step 7;
- it can cause great damage to the system but mainly in combination with an external attack.

FR - The reaction force of step 7 Security is :
- made from the calculation of the system itself in the design phase;
- based on internal protection resources;
- usually given by the IT equipment of the system;
- the first system left behind from a technological point of view;
- one of the major consumers of system resources.

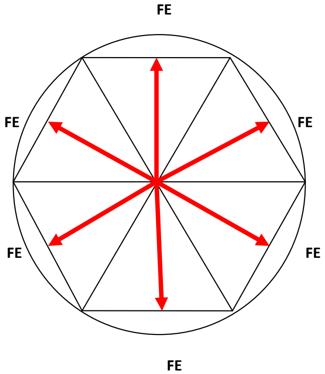

Fig 5. Scenario 3: The natural tendency of each internal system to become dominant relative to the others within any sum of systems that make up a defined whole system
Source: Author

FE - the balance force is:
- equal in all equilateral triangles representing the six steps of a BPR Business Reengineering Plan;

- theoretically equal in size to the apex of the hexagon in case of leakage of information inside the system as in the case of the scenario;
- is equal to the radius of the circle in the case of an attack on the system executed from outside it as in the case of scenario 2;
- in the situation of the analysis of the BPR itself as a global mechanism or system the apotheosis is the force of the general system that must maintain the internal balance of the system;
- in the case of the step analysis itself as a subsystem visualized by the equilateral triangle is equal to the geometric height;
- the force that plays a major role in maintaining the internal balance of the six steps of the BPR, due to the natural tendency of each internal system to try to develop to the detriment of the others. A BPR is an obvious disruptive factor of the already disturbed system from its equilibrium state, a system that the team that performs, implements and verifies seeks to restore it to its previous equilibrium state. In the following we will study the resilience of the system proposed by the theory launched above and for this:

1. We will first define the term resilience as c the ability of someone to return to normal after suffering a shock, in our case an economic shock[1] **.**
2. We will name the vertices of the equilateral triangle as follows:

   A) culture: in our case the organizational culture of the society subject to reengineering;

   B) environment, entering here:

   - the material basis of the company subject to reengineering;
   - business environment.

   C) knowledge, in our case:

   - principles and levels of Knowledge;
   - its implementation (including the employee's conscience, the process of knowledge, etc.) within the company subject to reengineering. Since it is an equilateral triangle, it is obvious that in order to respect the equilibrium and maintain the evenness of the triangle , the point of intersection of the forces generated (assimilated to the important lines of the equilateral triangle) by each vertex of the triangle will always be the same . and located in the center of gravity of the figure[2].

3. Considering that the need for reengineering is precisely due to the disruption caused to the system by one of the three forces corresponding to each angle, in order to respect the equilibrium of the company subject to reengineering - ie for

[1] https://dexonline.ro/definitie/rezilienta, (20.02.2022)

[2] Property 3. In an equilateral triangle, the center of the circumscribed circle coincides with the center of the inscribed circle, the orthocenter and the center of gravity , https://liceunet.ro/ghid-geometrie/coliniaritate-concurenta-paralelism/centrul-cercului-circumscris- sylvester's relationship, (18.02.2022)

the success of the proposed plan , it will have to act accordingly. For this, each of the 3 components will first be analyzed in the steps in the number 2 and 4 of the BPR, respectively and Depending on the result of the analysis, action will be taken on them to restore the steady state.

We will calculate the BPR identity resilience index IRI. To do this, we must first specify the indicators for each corner of the figure, indicators that must be considered when establishing the mathematical relationship to define the equilibrium of the company/business subject to BPR. Thus, we will have:

The sum of indicators related to organizational culture and measuring confidence **Σ I:**

A) - confidence in the management of the company ;

- business confidence ;
- level of employee satisfaction;
- confidence in the new business processes proposed by BPR ;
- the degree of community / brand cohesion of employees subject to BPR;
- the level of multiculturalism existing in the society subject to BPR .

B) The sum of the indicators related **to** knowledge Σ **ICU**- the development index of new technologies and processes proposed by BPR ;

- degree of use of foreign languages;
- number of unskilled, skilled and highly qualified employees.

C) Sum of environmental indicators **Σ IM**:

D) the level of SAB budget allocations with an impact on employees proposed by BPR;

- the level of SAB budget allocations with an impact on the endowments proposed by BPR;
- restrictions/facilities imposed/brought by recent amendments to laws, regulations, etc. at local, national, international level but with a direct or indirect impact on the business.

The equation of the IRI IDENTITY RESILIENCE INDEX of the **IRI** BPR, practically the equilibrium of the analyzed business system will be, taking into account the proposed mathematical model of the equilateral triangle, the following:

$$\boldsymbol{IRI} = \frac{\Sigma\ \mathbf{IC} + \Sigma\ \mathbf{ICU}}{\mathbf{2}\Sigma\ \mathbf{IM}}$$

We will use for the identity resilience index of a BPR the value **1** as maximum and which value corresponds to an ideal situation in which the company made profit, fulfilled its projects, employees and suppliers were paid etc and **0** as the minimum value corresponding to closing the business.

Due to the fact that the angles are equal in the equilateral triangle and each value of each sum must be equal to either of the other two, regardless of the number, importance, value and size of the indicators that make up the amount in question:

Σ IC = Σ ICU = Σ IM

It is also obvious that by respecting this formula the value **0** theoretically cannot be reached within a BPR which leads to the following conclusions:

1. A BPR cannot be considered to have zero value .
2. The 3 determining values in a resilience calculation of a BPR (culture, environment and knowledge) are those that encompass both the material and immaterial aspects of a business.
3. The role of an BPR is to restore the uncontrolled disturbed system, identified as the business itself , to equilibrium by producing a controlled disturbance but[1]
4. Any BPR is subject to a state of resilience identified by the 3 components mentioned above, which only in balance can ensure the success of the process.

Conclusions

1. Reengineering is a means of action and reaction of neoliberalism of great relevance and widespread in the world economy.
2. Management reengineering and/or management reengineering at the organizational/corporate level is one of the major challenges facing the shareholders/owners of a company that wants to execute such a process today.
3. The protection of information and the lack of guarantee of its security within the concept of reengineering, especially in the conditions of today's society (characterized by serious economic effects caused by crises, pandemics, cyber attacks, etc.), is one of the great unresolved problems of reengineering but and the major reason for the distrust of employees in companies subject to this process.
4. As a solution we propose the introduction in the Reengineering Plan of a new step, called security along with the seven steps of classic reengineering, in view of the need to ensure information security during the process, a step that thus becomes conditional.
5. Osiceanu's theory on the seven steps of reengineering in terms of information security in such a process introduces, describes, motivates and justifies the need for the new step security.
6. The lack of a separate research topic related to the introduction in a BPR of an analysis of the resilience of the business subject to this process, the execution of a resilience plan, etc. is, in our opinion, one of the causes of the high failure rate of reengineering.
7. At the same time, the stability of the BPR is characterized by a state of resilience, based on the balance of three components: organizational culture/trust, team professionalism and technological level appropriate to the legal environment, which only in reciprocal balance can ensures the success of the process.

[1] John Naisbitt, *Megatendinte*, Politica, București, 1984, p.79

Theme 1: Protection and guarantee of information in a system subject to reengineering	**The specific objective (OS)**	**Research hypothesis (I)**
	OS 1. 1. Identifying the information, the way of collecting, transmitting, analyzing, using, storing, reintroducing its use,	***I.1.1.*** Shortcomings of the reengineering process in ensuring the security of the information provided in an BPR
	OS 1.2. Analysis of existing methods of protection and assurance of information security in a system subject to reengineering	***I.1.2.*** Lack of information security reengineering in a BPR
	OS1.3. Introducing new approaches to information security and information security in a reengineering process	***I. 1. 3.*** The possibility of completing the theories of information and reengineering through the Osiceanu Theory on the seven steps of reengineering

Tab. 1. General Dashboard of Theme 1: Protection and guarantee of information in a system subject to reengineering
Source: Author

Specific objective OS 1.1. Identification of information, of the way of collection, transmission, analysis, use, storage, reintroduction into use of it, Hypothesis I.1.1. Shortcomings of the reengineering process in ensuring the safety of the information provided in a BPR.

Theme 1: Protection and guarantee of information in a system subject to reengineering			
OS 1. 1. Identifying the information, the way of collecting, transmitting, analyzing, using, storing, reintroducing it into use,	***I. 1. 1.*** Lack of the reengineering process in terms of ensuring the security of information provided under an BPR		
Questionnaire	Result	Measurement method	Research variable
1. Are there any gaps in the security of information provided in an BPR or not ?	Yes: 306 No: 144	Open question (Yes/No)	knowledge of the concept and the law
2. He is considered to be the strongest who; A) holds the information and cannot use it B) stores the information and can use it whenever needed ?	A: 221 B: 229	open question (Yes/No)	knowledge of the concept
3. The legal framework for information security is established in Romania by : A) law B) internal documents	A: 312 B: 138	open question (Yes/No)	knowledge of the concept and the law

4. The information provided in a BPR in Romania is: A) protected by specific laws and regulations B) unprotected	A: 378 B: 72	open question (Yes/No)	knowledge of the concept and the law

Tab. 2. General Dashboard of Theme 1: Protection and guarantee of information within a system subject to reengineering,
Source: Author

A) ANOVA dispensational analysis of the specific objective OS 1.1; identification of information, of the way of collecting, transmitting, analyzing, using, keeping, re-entering into use thereof. Case 1: Results of the questions according to the answer criteria (yes/A): 306, 221, 312, 378. Case 2: Results of the questions according to the answer criteria (no / B): 144, 229, 138, 72.

Anova: Single Factor

SUMMARY

Groups	*Count*	*Sum*	*Average*	*Variance*
Cazul 1	4	1217	304,25	4144,25
Cazul 2	4	583	145,75	4144,25

ANOVA

Source of Variation	*SS*	*df*	*MS*	*F*	*P-value*	*F crit*
Between Groups	50244,5	1	50244,5	12,12391	0,013111	5,987378
Within Groups	24865,5	6	4144,25			
Total	75110	7				

Tab. 3 ANOVA dispensational analysis of the specific objective OS 1.1

In the ANOVA table, Statistics **F=12.12391** are calculated with a value **p=0.013111** (materiality threshold). This p-value allows us to say that at least two environments differ significantly (with a probability of 95%), which means that the chosen tactic is appropriate and thus the hypothesis is validated.

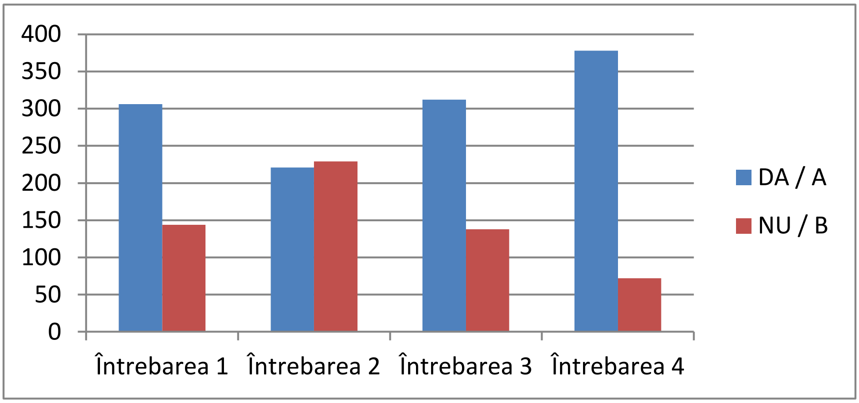

Fig. 6. Graphical representation of the result of the questionnaire for Theme 1, Specific objective OS 1.1, Hypothesis I. 1.1.
Source: Author

Analysis of existing methods of protection and guarantee of information security within a system subject to reengineering, Hypothesis I.3.2.; shortcomings of the reengineering process in the field of the security of information provided within the framework of a BPR

Theme 1: Protection and guarantee of information in a system subject to reengineering			
OS 1. 2 . Analysis of existing methods of protection and assurance of information security in a system subject to reengineering	***I. 1. 2.*** Lack of information security reengineering in a BPR		
Questionnaire	Result	Measurement method	Research variable _
1. Are current methods of protecting and ensuring the security of information in a system subject to reengineering sufficient ?	Yes: 336 No: 114	question (Yes/No)	knowledge of the concept
2. Is there a model model for regulating the protection and guarantee of information security in a system subject to reengineering ?	Yes: 53 No: 397	question (Yes/No)	knowledge of the law
the method of hiring ORNISS accredited personnel in airlines of national interest or with state capital correct even if it involves higher costs ?	Yes: 276 No: 174	question (Yes/No)	knowledge of the concept
method of employing accredited personnel in national or state-owned airlines ORNISS ensures fully protected a _ and ensuring the security of information in a reengineering system ?	Yes: 392 No: 58	question (Yes/No)	knowledge of the concept
5. Do the companies that ensure the creation and implementation of a BPR guarantee the	Yes: 403 No: 47	question (Yes/No)	knowledge of the

protection and security of the information received ?			concept and the law

Tab. 4. General Dashboard of Theme 3: Protection and guarantee of information within a system subject to reengineering, Specific objective OS
Source: Author

ANOVA dispensational analysis of the specific objective OS 3.2.; analysis of existing methods of protecting and guaranteeing the safety of information within a system subject to reengineering.

Anova: Single Factor

SUMMARY

Groups	*Count*	*Sum*	*Average*	*Variance*
Cazul 1	5	1460	292	20408,5
Cazul 2	5	790	158	20408,5

ANOVA

Source of Variation	*SS*	*df*	*MS*	*F*	*P-value*	*F crit*
Between Groups	44890	1	44890	2,199574	0,176337	5,317655
Within Groups	163268	8	20408,5			
Total	208158	9				

Tab. 5. Case 1: Results of the questions according to the answer criteria (yes): 336, 53, 276, 392, 403. Case 2: Results of the questions according to the answer criteria (no): 114, 397, 174, 58, 47

In the ANOVA table, Statistics **F=2.199574** are calculated with a value **p=.176337** (materiality threshold). This p-value allows us to say that at least two environments differ significantly (with a probability of 95%), which means that the chosen tactic is appropriate and thus the hypothesis is validated.

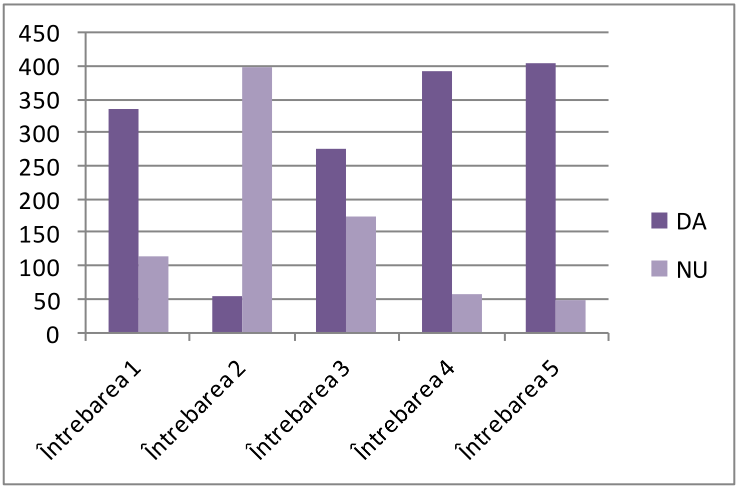

Fig. 7. Graphical representation of the result of the questionnaire for Theme 1, Specific objective OS 1.2, Hypothesis I. 1.2.
Source: Author

Theme 1. Protection and guarantee of information in a system subject to reengineering			
OS 1.3. Introducing new approaches to information security and information security in a reengineering process	***I.1.3.*** The possibility of completing the theories of information and reengineering through the Osiceanu Theory on the seven steps of reengineering		
Questionnaire	Result	Measurement method	Research Variable
1. Is there a need to complete current procedures and applications for information security and information security in a reengineering process?	Yes: 241 No: 209	Question (Yes / No)	knowledge of the concept and the law
2. Does the general theory of reengineering introduce a specific step strictly related to the subject of information security and information security in an BPR, increase its degree of success?	Yes: 317 No: 133	question (Yes / No)	knowledge of the concept and the law
3.Due to the specificities of the field of civil aviation in which the members of the reengineering teams are linked both to the companies subject to this action and to the competing companies through their past, relatives, etc. , as part of a reengineering process by introducing in the general theory of reengineering a specific step strictly related to the subject of security information and	Yes: 339 No: 111	Question (Yes / No)	knowledge of the concept and the law

information guarantee within an BPR?			

Tab. 6. General Dashboard of Theme 1: Protection and guarantee of information in a system subject to reengineering, Specific objective OS 3.3. Presentation of new approaches to information security and information assurance in a reengineering process, Hypothesis I.3.3.
Source: Author

ANOVA declensional analysis of the specific objective OS3.3.; presenting new approaches to information security and guaranteeing information in a reengineering process

Anova: Single Factor

SUMMARY

Groups	*Count*	*Sum*	*Average*	*Variance*
Cazul 1	3	897	299	2644
Cazul 2	3	453	151	2644

ANOVA

Source of Variation	*SS*	*df*	*MS*	*F*	*P-value*	*F crit*
Between Groups	32856	1	32856	12,42663	0,024337	7,708647
Within Groups	10576	4	2644			
Total	43432	5				

Tab. 7. Case 1: Results of the questions according to the answer criteria (yes): 241, 317, 339. Case 2: Results of the questions according to the answer criteria (no): 209, 133, 111.

In the ANOVA table, the statistics **F=12.42663** are calculated with a value **p=0.024337** (materiality threshold). This p-value allows us to say that at least two environments differ significantly (with a probability of 95%), which means that the chosen tactic is appropriate and thus the hypothesis is validated.

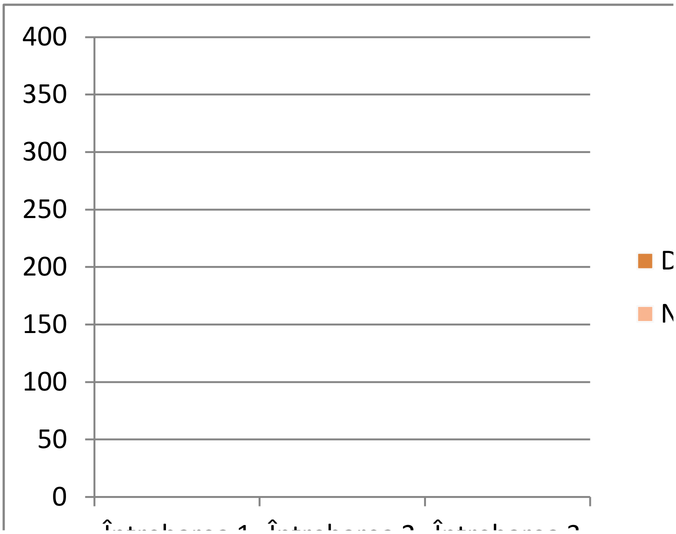

Fig. 8. Graphical representation of the result of the questionnaire for Theme 1, Specific objective OS 1.3, Hypothesis I. 1.3.
Source: Author

The sampling method used was applied on the basis of a random choice to a sample of a selected group. These samples therefore responded to the selection request by completing a questionnaire . The selection was attended by people of different ages, of different sexes and of different professions, who work or have worked in the field of civil aviation, as well as others who had access to related information in the field of civil aviation.

The selection method is part of the category of statistical selection where numbers of people were used as input data according to clearly established criteria and as output data were the graphs of the samples used in the approach of the established criteria.

Bibliography

Books

1. Hammer,Michael; Champy, James, *Reengineering the Corporation: A Manifesto for Business Revolution*, Harper Collins Publisher, New York, 2006
2. Smith, Adam *The Wealth of Nations,* Chapter I - Of the division of labor, Wordworth, Stansted, 1776
3. Fayol, Henry, *General and Industrial Management*, Dover Publication, Mineola New York, 1949
4. Koestler, Arthur *The Ghost in the Machine* , Hutchinson, London, 1967
5. Davenport, Thomas H.; Gilbert, J.; Probst Heinrich von Pierer, *Knowledge*
6. *Management Case Book*, , 2nd Edition, Siemens Best Practice, 2002
7. Petrescu, M.; Petrescu, A.G.;Fl. Bilcan, R.; Camarasan, V.A, *Tools and*

8. *mechanisms regarding the management of classified information – From theory to practice*, Biblioteca Targoviste, Editura, Locul, 2017
9. Cioban Petre; Burlan Daniel, *The New Criminal Code*, Rosetti International, București, 2020
10. Naisbitt, John, *Megatendinte*, Politica, București, 1984
11. Champy James, *Engineering the Corporation: Reinventing Your Business in the Digital Age*, Warner Books, New York, 2002
12. Davenport, Thomas H., (2003), *Process innovation: Reegineering Work through Information Technology*, Harvard Business School Press, Boston, 2003

Articles and Studies

1. Al-Mashari, Majed; Zairi, Mohamed, *Revisiting BPR: a Holistic Review of Practice and Development,* ”Business Process Management Journal”, March 2000
2. Attaran, Mohsen; Wood, Glenn, *How to Succeed at Reengineering*, ”Journal of Management Decision”, vol. 37, No. 10/1999

Documents

1. *Law 182 / 12.01.202 Regarding the protection of classified information*, Monitorul Oficial no. 248 / 12.04.2002
2. *Law 51/1991 on the National Security of Romania*
3. *Law 544 / 12.10.2001 Regarding the free access to information of public interest,* Monitorul Oficial no. 663 / 23.10.2001
4. *The Romanian Constitution*

Websites

1. https://gdpr.eu/
2. https://liceunet.ro/
3. https://dexonline.ro/
4. https://www.bhudeb.com/
5. https://www.emerald.com/