DOI: 10.2507/30th.daaam.proceedings.142

THE INFORMATION SECURITY TO SOFTWARE OF CRISIS MANAGEMENT

Marta Blahova, Vaclav Mach, Lukas Pavlik, Martin Hromada & Ficek Martin

This Publication has to be referred as: Blahova, M[arta]; Mach, V[aclav]; Pavlik, L[ukas]; Hromada, M[artin] & Ficek, M[artin] (2019). The Information Security to Software of Crisis Management, Proceedings of the 30th DAAAM International Symposium, pp.1019-1025, B. Katalinic (Ed.), Published by DAAAM International, ISBN 978-3-902734-22-8, ISSN 1726-9679, Vienna, Austria
DOI: 10.2507/30th.daaam.proceedings.142

Abstract:

This paper deals with security of information in crisis management software. The paper defines types of information in the crisis management and categorizes these according to the needs of protection. In the next part it deals with the crisis management software itself. The paper defines sixt areas according to determination of the appropriate software and engages in relation between these software and information. The paper specifies what software works with what information. The paper works with COBIT methodology, COBIT cube and up to some extent with SWOT analysis. There are discussed particular elements of the COBIT cube and they are applied to the problematics of the crisis management software. The paper demonstrates relations between particular elements of the COBIT cube through examples of the application of the COBIT cube to the problematics of the crisis management software and shows difficulties and problems associated with this.

Keywords: COBIT; crisis management; software; information; security.

Introduction

What information is used in crisis management? What information is relevant to crisis management software? How is the information protected? The article tries to find answers to these questions. The article will deal with the classification of information, information handling and storage, everything will focus on the area of crisis management in state administration and specifies the area of software for crisis management. It should be noted at the outset that even such a specified area is quite broad and although the article in the following pages will try to describe the whole level of the issue, it may happen that some aspects or areas of this issue are omitted. However, this is not because the authors do not want or omit to include the aspects or areas in question, but simply because the article is so extensive that its basic meaning, which is a brief summary of the issue, is lost.

1. Information in crisis management

At the beginning of this section, it should be noted that in the area of crisis management in state administration and self-government, there is information included in the special regime. This is classified (reserved) and sensitive information. We will not deal with classified information in the case of software used in crisis management. Yet the definition of reserved information is. "Reserved information is information if disclosure to an unauthorized person or abuse may be disadvantageous to the interests of the Czech Republic." [1]

Another category, as already mentioned, is sensitive information. In general, it is: "non-public information that requires protection because unauthorized disclosure, use, alteration, loss or destruction could cause damage to the person or institution to which it relates. The basic categories of sensitive information are personal data (eg health), economic data (commercial, industrial, service, banking, etc.) and data relevant to the security of the state (state secrets, classified information). "[2]

We can further divide this sensitive information:

1) Information covered by the obligation of confidentiality.
2) Personal Data - Protected by Act no. No. 101/2000 Coll., on the protection of personal data.
3) Special facts - Protected under Act no. No. 240/2000 Coll., Crisis Act.

Regarding specific information in crisis management software, we can divide the information:

1) Graphic information.
2) Information written.
3) Audio information.

These are various information in digital form such as map background, written messages, voice recordings and so on. The relevant information for the software is then selected from the general crisis management information. This part should serve as a basic introduction to information in crisis management.

2. Crisis management software

There are a lot of software that uses crisis management because the issue of crisis management is quite wide. Leaving aside software of an administrative nature, such as the accounting system, there will be software specialized for crisis management purposes and software usable for crisis management purposes. For example, software Aloha, Terex, Posim, Recovery, IVVS, Argis, etc.

For clarity, we can divide them into several groups according to their focus and use, they are it:

1) Geographic information systems.
2) Modeling and simulation systems.
3) Monitoring systems.
4) Communication systems.
5) Special database KŘ.
6) Next

Although this division is quite simplistic, it is for understanding the substance sufficient.

Types of crisis management software and relationship to information.

This section will describe the type of information that each type of crisis management software deals with. It should be noted that each of these systems works with databases, but there are also specific database systems in the area of crisis management and are therefore listed as a separate group.

Geographic information systems - These systems work with graphical information (map background, pictures and more), written information (in the database, such as shelter locations, civil protection squads, etc.) and some systems also with audio information.

Modeling and simulation systems - These systems work with graphical information (maps, pictures and more), written information (information necessary for the actual modeling and simulation eg procedures of IRS components, information obtained from measuring stations, etc.) and some systems with audio information (eg. recorded audio notifications etc.).

Monitoring systems - These systems work with graphical information (pictures, camera recordings and others), written information (information obtained from measuring stations or information obtained by measurement and entered into the system, etc.).

Communication systems - These systems work with graphic information (images, camera recordings and other transmitted graphic information), written (various written information transmitted) and of course audio information (voice transmission, audio recordings and the like).

Special Crisis Management Databases - These systems work with graphical information (Graphical information necessary for the functioning and effectiveness of the system), written (information in the database, such as shelter locations, civil protection traits, number of units, unit equipment, etc.) audio information.

Others - These systems work with graphical information (maps, pictures and more), written (information in the database, such as decisions of the governor, executive orders, etc.) and some systems also with audio information.

COBIT methodology

For the purposes of this article the COBIT methodology will be used, ie Control Objectives for Information and Related Technology. "This is a set of generally accepted processes, assessment guidelines, indicators and best practice to maximize the benefit of an organization's IT benefits." [3]The basis of this methodology is a tool called COBIT cube. This tool works with organizational goals (strategic requirements), IT resources and processes.

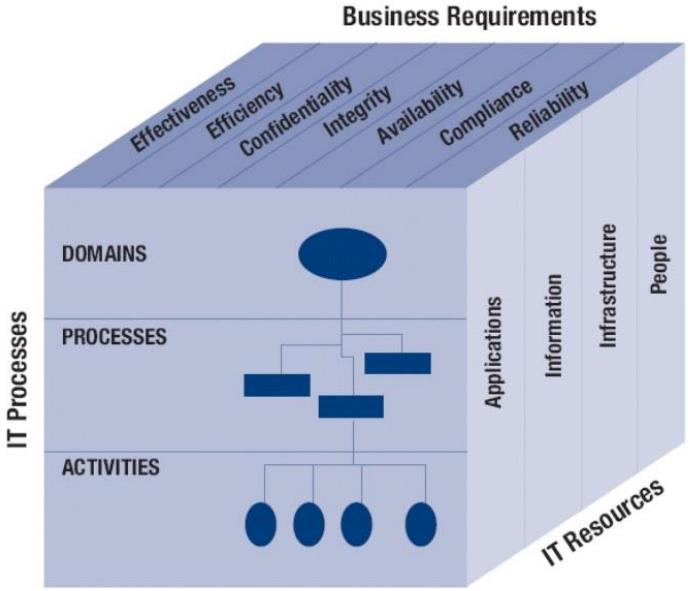

Fig. 1 - COBIT Cube[4]

3. Resources in crisis management software

The basic sources are applications, information; infrastructure and people. When we define resources, it is important to realize that software itself is an application. For this reason, the application source can be omitted. Since we are speaking on a general level, we can only summarize at the point of information that we have graphical information, written information, audio information. As far as infrastructure is concerned, we focus primarily on hardware and software distribution itself, ie whether it is client-server software or workstation software. Lastly, there are people who have a significant impact on security.

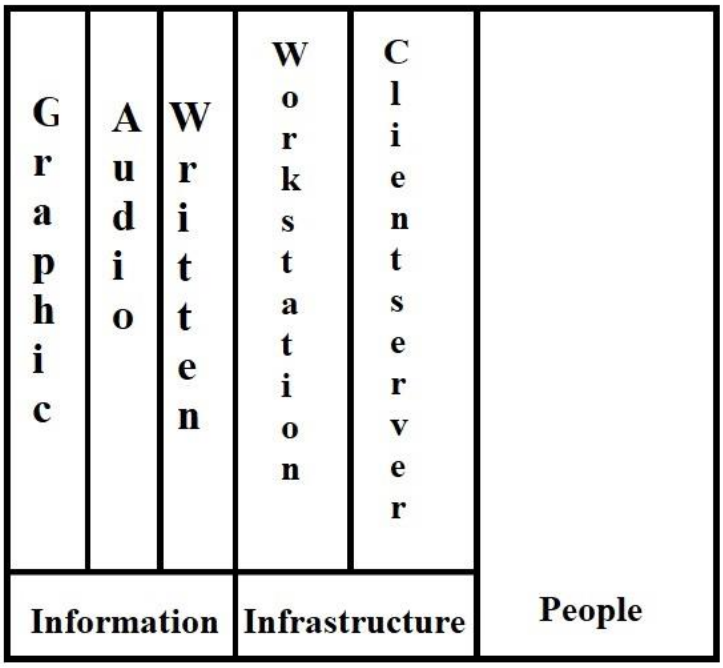

Fig. 2 - Page resources from COBIT cubes. Source: Own

To better understand the issue of resources will be used SWOT analysis, which defines strengths, weaknesses, opportunities and threats.

SWOT	**Auxiliary**	**Noxiously**
Internal origin (based on the software itself and its environment)	Strengths: Increased security of rooms with appropriate workstations	Weaknesses: Lower literacy of workers in the sense of security and information.
Outdoor origin(non - influences) software and its environment)	Opportunities: Use of modern technology	Threat: Blackout .

Table 1. SWOT analysis in SW. Source: Own

Since the SWOT analysis is intended only to demonstrate some selected aspects it is not it needs to be analyzed in more detail or quantified.

4. Information criteria

The basic information criteria are efficiency, performance, confidentiality, integrity ,availability, compliance, authenticity. When we talk about efficiency, we mean the criterion of usefulness, that is, how it is givensoftware, or a single process beneficial to the task. In most cases in this. The area is meant how relevant information the software is able to provide. The criterion of performance in this area is mostly the time it takes for software able to manage the entered information and provide output. The criterion of confidentiality is partly meant by security itself, as it is here o the ability of the software to provide correct and appropriate information. Here is a significant proportion security, because only if the software is sufficiently secure can it work properly without fear of attacking and resulting data degradation.

Only if the integrity of the whole system is respected can it function properly and fully from this for this reason, this criterion ranks among the most important yen. Availability, this parameter is largely influenced by software design and destination of the software itself, it is clear that the availability of communication software is more significant than GIS software. But here we have to realize that availability is not just parameter of the whole software or information, but

the individual parts of the software, it is closely related with the integrity criterion. Conformity is a criterion that can be understood as the ratio between intention, project and the facts. It is not often that the ratio is 100%. It may be difficult to reach agreement between the project and the project (s), and it is even harder to reach agreement between the project and the project facts. Here we perceive the project as a proposed system, however, not yet implemented theoretical.

Authenticity, like any of the parameters described above, can also be this parameter apply both to individual parts of the system and to the system as a whole, or its resources and processes, however, this parameter is most important for output information. In practice, for example it happens that two modeling and simulation software will produce diametrically different results Such a thing is quite unpleasant. If the crisis worker is to decide on the extent of evacuation, needs credible information, and this is the criterion for software used in crisis management is particularly important for output information. [6]

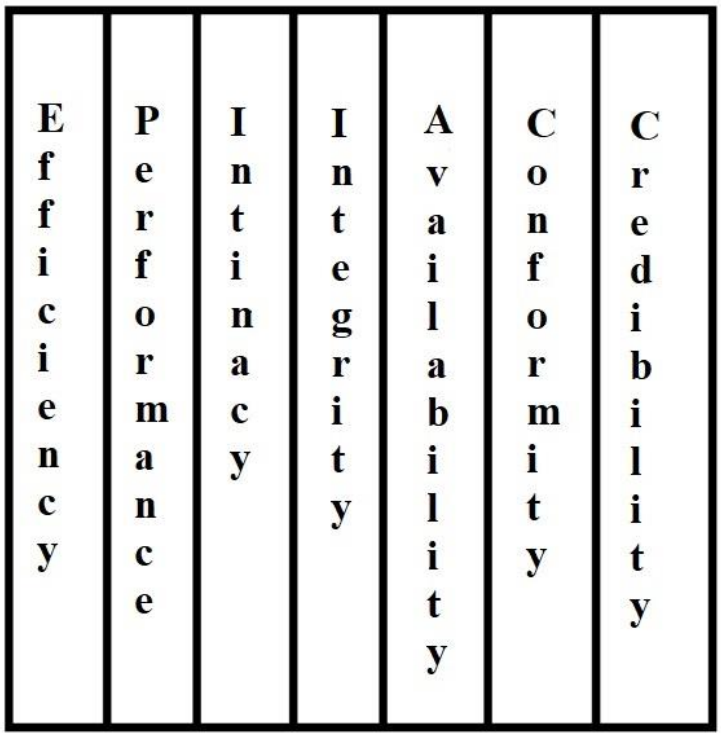

Fig. 3 - Page of criteria from COBIT cubes. Source: Own.

5. IT processes

IT processes are the most complex element that is very difficult to define. IT processes up consist of domains, processes, and activities. Generally, domains can be identified, including planning and organization, acquisition and implementation, delivery and support, and tracking and evaluation. [3]

Domains then use processes that use activities. Processes and activities are in methodology A number of COBITs have been defined and it would be burdensome to address them for the purposes of this article. Since we are talking about several types of software, it is not easy to identify precise processes and activities. In general, it can be said that these will be processes: information storage, work with information, displaying, data transfer, input of information etc. Of course it would be possible find more processes, but it is enough to illustrate. These processes are further divided into activities.

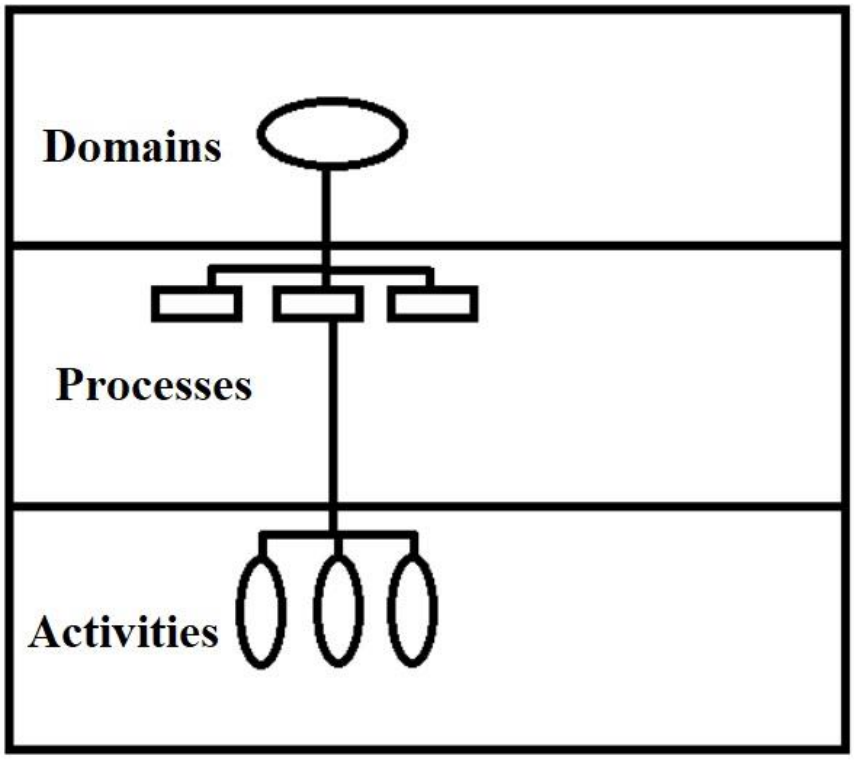

Fig. 4 - The side of IT processes from COBIT cubes. Source: Own.

6. Cube COBIT

In this section of the article, the resources, criteria, and processes described above will be applied and Shown with COBIT cubes. It is good to realize that resources are managed by processes in order to achieve objectives meeting the criteria. [5] [6] In order to achieve the best possible condition it is necessary to apply in each domain adequate processes and activities that will work with resources, in this case with information either graphical, written or audio infrastructure, either on the workstation or client basis server and human resources, so that the resulting goals are in accordance with the criteria, performance, confidentiality, integrity, availability, compliance and authenticity. [7] [8]

For example, an acquisition domain might be a simplified example and implementation, in this domain there are, inter alia, processes of software acquisition, its implementation, collection of relevant data, their sorting and subsequent insertion into the enterprise, but also training of workers and others. These processes then develop other activities, such as the collection process relevant data will be used for example activities, obtaining information from experts, data collection from the general public, collecting data from a variety of registers, and so on information, but we also work with information as a source (for example, work with the information in the form of a list of experts to contact, etc.) we use the resource infrastructure (databases can be our own, for example, a list of experts in the form of Excel tables (workstation, central registers on the client-server principle) and last but not least human resource. [10]

We manage these resources in processes and activities so that they meet the criteria as much as possible. An example would be the efficiency criterion in the process of gathering information activity gain information from experts. Here we will use effectively relevant information, so instead of a list hiding places we use the list of experts, which, as you will recognize, will be more effective. Because already such a list is made and stored on the workstation, so we will use it just now a workstation rather than a client-server infrastructure that runs, for example, central registers, and we would have to look for individual experts. As you will recognize, this procedure is more efficient. Last but not least, we will use qualified workers for such collection an act, such as a crisis management officer who has the knowledge and skills to collect the type of information required. This is also more effective. It is understandable that in fact the whole issue is more complex, but for understanding these examples will suffice.

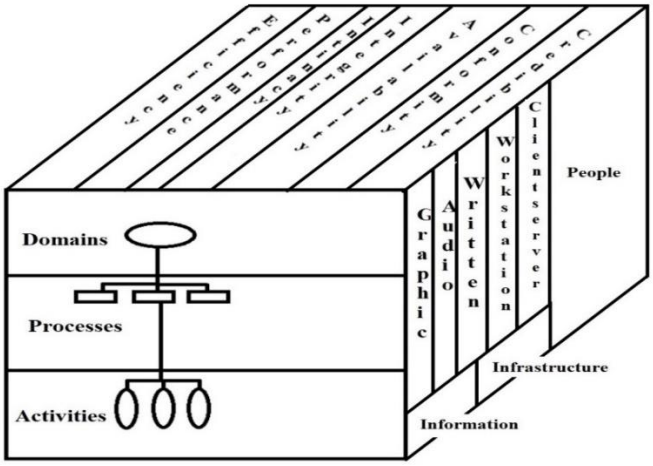

Fig. 5 - The resulting COBIT cube. Source: Own.

7. Conclusion

Due to the general direction of this article, it is difficult to determine a clear measure information security in crisis management software. It should be said that the current software Crisis management are already secured at a high level, but there is always something to improve, indeed how it also shows the PDCA method (plan, do, check, act), which is based on most methodologies built. This article deals with information security in crisis management software. They were specified information in crisis management and categorized according to their security needs to information subject to confidentiality, personal data, special facts and classified information. Further, the information was divided according to the form into graphic information, written information, audio information. Software was divided into geographic information systems, modeling systems and simulation, monitoring systems, communication systems, special database of crisis management and other. The relationship of information to these software has been described. The article briefly described the methodology of COBIT and COBIT cube and partially applied it to in the field of crisis management software. For this issue were defined resources, and form The examples outlined the links and some problems. Finally, it is necessary to point out that this area is complex and complicated and dynamically growing and therefore it is necessary to constantly monitor it and look for ways to this area improve. This article can serve as an introduction to the issue and outlines possible others developments which may include, inter alia, raising information security awareness in crisis management, both in general and directly in crisis management software.

8. Acknowledgments

This research was based on the support of the Internal Grant Agency of Tomas Bata University in Zlín, the IGA / FAI / 2019/003, IGA/ CebiaTech/ 2019/003 project and the Institute of Security Engineering, Faculty of Applied Informatics.

9. References

[1] Czech Republic. (2005) Act on Protection of Classified Information and Security Act. Collection of Laws. Prague: Ministry of the Interior, 143/2005, 412/2005.
[2] Sensitive Information. (2012). KTD - Czech Terminological Database of Librarianship a Information Sciences (TDKIV). Prague: ExLibris, NL CR. Available from: http://aleph.nkp.cz/publ/ktd/00000/03/000000388.htm
[3] Doucek, P., Novák, L. & Svatá, V. (2008). Information Security Management. Prague: Professional Publishing. ISBN 978-80-86946-88-7.
[4] Cobit, (2014). Iowa state university. Ames: Iowa State University of Science Technology. Available from: http://www.internalaudit.iastate.edu/internalcontrols/cobit
[5] Cobit (2015). Systemonline. Prague: CCB spol. s r.o. Available from: https://www.systemonline.cz/sprava-it/cobit-5-vmalych- a-medium-firm.htm
[6] Požár, J. (2005). Information security. Pilsen. University textbooks. ISBN 80- 868-9838-5.
[7] Blistanova, M. (2014). Data Preparation for Logistic Modeling of Flood Crisis Management. In: 24th DAAAM International Symposium on Intelligent Manufacturing and Automation, 2013. Vienna, 1529 – 1533. ISBN 1877-7058.
[8] Smith, R. (2016) Elementary information security. Second edition. ISBN 12-840- 5593-0
[9] Whitman, M. & Mattord, H. (2016) Principles of Information Security. Fifth edition. ISBN 978-128-5448-367.
[10] Drastich, M. (2011). Information Security Management System. Prague. Travel Guide. ISBN 978-80-247-4251-9.
[11] Lidinsky, V., Svarcova, I., Budis, P., Loebl, Z. & Procházková, B. (2008) EGovernment safely. Prague: Grada. EAN 24763552.