SELECTED PROBLEMS OF INFORMATION CONTINUITY FUNCTIONING OF CRISIS MANAGEMENT SYSTEMS IN THE ASPECT OF USING SERVICES IN CLOUD COMPUTING

Włodzimierz Miszalski

Wojskowa Akademia Techniczna

Wojciech Zaskórski

Wojskowa Akademia Techniczna

Abstract. Cloud computing services constitute current proposal for virtualization of activities and integration of different processes dependent on access to information resources. Cloud computing services may eliminate access barrier and make it possible to use information resources in internal and external relations for crisis management systems and crisis response systems. CC services can strengthen organization potential and can help to improve information continuity by using many proved and advanced applications.

Key words: Business continuity, Information based continuity, Crisis management systems, Cloud computing, Crisis, Information security, Virtualization of information resources, Services in cloud

Introduction

Standards in the 21st century as well as dynamics of political, economic and technological phenomena indicate the need for special care concerning information resources and access with taking into account timeliness, completeness and coherence criteria. Effective use of both internal and external resources results in an improvement of potential of every operating (organisation) system and creates a specific value added chain. In case of contemporary organisations, including crisis management (response) systems – perceived as collection of organised processes performed in close connection with the environment – information continuity becomes one of the most significant criterion. Threats to the above-said continuity will imply a certain level of risk. That risk will, at the same time, determine a level of security.

Functioning of every organization under the condition of the loss of information continuity requires a special manner of perceiving as well as protecting information resources. It concerns also the entire range of critical infrastructure, including ICT systems and networks [9, 10]. It shall mean striving to improve the quality of functioning with keeping the criterion of maximum effectiveness under certain circumstances. One of significant manners of searching a solution which will improve the effectiveness of the information resources use in crisis management systems is “cloud” computing [3] defined as a possibility to access technical and technological resources (including information) – perceived in terms of services – as well as possibility to use this platform in order to increase own resources (performance) with keeping the criterion of continuity of functioning [4, 5].

1. Organisation functioning continuity in crisis situations

Criterion of business continuity shall mean in particular care for fulfilment of all the conditions enabling performance of the statutory tasks of every organisation. Critical infrastructure is a potential, which should guarantee the above-said continuity at the basic level. In fact internal potential of every organisation is limited to a significant extent. Therefore, the use of resources of the environment should result in potential increase as well as improvement of the level of business continuity in emergency situations, in different types of failures and crisis situations [20]. The range of negative processes and their consequences concerning the entire organisation will probably differ and will depend on both a particular threat and its possible transfer to other components/subsystems in a particular organisation. Every operating system (every organisation) is characterised by specific level of tolerance to a particular type of risk. It is conditional upon the quality of particular components (subsystems).

Environment is usually a potential source of crisis both as far as the forces of nature are concerned, but also in the sphere of politics and culture, as well as technology itself, which includes the phenomenon of cyber terrorism. However, an environment may be also perceived as the source of opportunities, increasing internal potential of a particular organisation. Every contemporary organisation, as a relatively isolated system, but an open one – is related to an external environment. This fact is essential for analysis of safety level of organisation, and, in particular, it influences the level of implementation of objectives according to determined operations strategy. Implementation of objectives under the conditions of significant indefiniteness and uncertainty[1]may be threatened. Sources of threats may be located internally and externally in case of every organisation. As mentioned beforehand – one of contemporary threats involves the area of information technology, and especially – ICT as well as relations resulting from it inside organisation, and relations with the environment. Those technologies constitute trouble spot of all management systems, including crisis management. Therefore, threats caused by damage or destruction (e.g. resulting from natural disasters, acts of terrorism or sabotage) to ICT infrastructure or prevention of access to information resources may be a sufficient reason for information discontinuity. Information discontinuity may directly violate organisational and material continuity.

[1] M. Kostera (red.), *Wprowadzenie*, in: *Nowe kierunki w zarządzaniu*, WAiP, Warszawa 2008, p. 23.

Specific character of functioning of each organisation depends on its structure, which results in necessity of dedicated approach to safety of a particular entity. It is worth noting that heading for process structures is determined by care for greater flexibility and smaller susceptibility to crises or typical threats. New sources of threats to the business continuity appear at the same time. The manner of actual management of a particular organisation shall determine all aspects, including precise management responsibility, resources management and monitoring as well as recording events and their results for the sake of current analysis and system improvement. Therefore we should base on sequence of processes and mutual interaction between them as well as uniform criteria and methods of ensuring their effective performance with the use of resources and information necessary for supporting the course and ensuring the business continuity.

Crisis situation and crisis are related to a certain type of anomalies disturbing normal operation of a particular entity. Business continuity may be disturbed in different spheres and its discontinuity may mean disturbance in operation in economic, social, technical and information spheres. Generally speaking, it may be assumed that crisis is a disturbance of the state of balance, with different scope and duration. Crisis and crisis situation are caused by different threats, including chance causes (natural) or assignable causes (intentional), which have an adverse influence on operation of a particular entity and / or cause adverse (or even dangerous) changes in its internal or external environment[2]. In case of threats to information resources and risk of loss of information continuity, potential actions of a man (or lack of certain actions) or influence of force majeure – may result in loss of a certain level of "skills" of technical resources, determining maintenance and release of relevant information or may cause decrease in the level of security in the sphere of loss of confidentiality, integrity or availability of relevant data and information. Then a necessity to identify losses, resulting from the importance of implemented project and the very critical process, becomes element of crucial importance[3]. In order to conduct a system threat assessment a uniform threats classification and characteristics[4] should be applied in a way enabling unambiguous taxonomy of threat types and categories as well as intensity of their performance in relation to the possibility of counteracting them. Both the criteria of threats division as well as threats categories directly illustrate a potential risk. Therefore the sources of threats, predicted period of their effects removal, threatened area and their predicted scope constitute significant criteria for

[2] K. Ficoń, *Inżynieria zarządzania kryzysowego. Podejście systemowe*, Wyd. Bel Studio, Warszawa 2007, p. 76.

[3] K. Liderman, *Initial identification of the term "natural disaster" and description of threats with particular focus on information security* (in the scientific research project PBZ-MNiSW-DBO 01/1/2007).

[4] The source: K. Ficoń, op. cit., p. 82.

taxonomy of threats to information resources. Categories of threats usually identify time, scope and their propagation area. Intensity of threats may indicate a periodical manner of threats appearance or their scalable value (small, average, high, great or unknown). As far as practical aspects of dealing with risk and threats to information resources are concerned [13, 15] it is worth to emphasize the reasons for risk of loss of information continuity, type of disaster or environmental actions, including the so called cyber terrorism.

2. Synchronization problems of crisis management decision cycle with the dynamics of crisis situation

The essence of crisis management is making decisions in a limited time and in changing dynamics and complexity of environment and organization. The decision maker's ability to control the organization depends upon the feedback received from the organization as well as upon the information acquired from the environment. The information delays make it harder for decision makers to understand the relationships that govern the dynamics and complexity of organization and environment in crisis situation. In the real crisis situations as well as during the exercises and simulation experiments we often see decision makers struggling to keep up with the pace of changes in the organization and environment. The delays occur on every stage of decision cycle (recognition, judgment, choice, execution, feedback) making it longer and non-stable.

Decision D(A) interpreted as a response to the current status A of organization and environment (Fig.1) is executed after certain time Δt. Meanwhile the status changes to B. In fact the execution of the D(A) influences the new status B the information on which has not reached the decision maker yet.

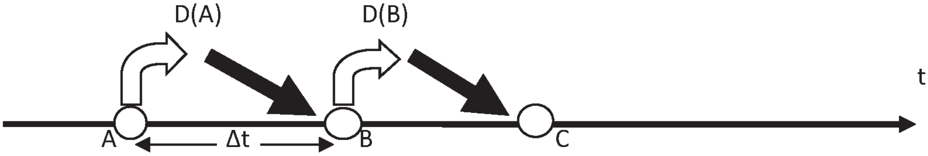

Fig. 1. Decision delay

Although most of decision makers realize the fact and try to synchronize the decision cycle with the dynamics of crisis situation it happens that the acceleration of the pace of status' changes makes the synchronization impossible. Implementing the delayed decisions may destabilize the organization and finally lead to the loss of functioning continuity.

3. Counteracting the loss of organization functioning continuity

Crisis management, including management of crisis response system should concentrate on the fact that it is a complex action/process included into the entire cycle of management under special circumstances, that is in the situation of risk or uncertainty[5]. Management of safety of information resources constitutes an integral element of information safety. Counteracting the risk of loss of information continuity is an activity consisting in restoration of normal condition (or maintenance of that condition), despite the occurrence of crisis situations and threats to the so called critical infrastructure [7]. The problem situation occurs when current condition of information resources and access to them differ from the desired condition[6] and either undertaking proper internal actions or the use of external resources is required. Therefore each organisation should ensure the conditions of effective activity, also in case of threats or crises occurrence. Such purpose may be obtained by means of creating an organisation security system, including a set of coherent measures and coordinated projects in order to ensure smooth course of the processes of collecting, maintaining, processing and revealing information[7].

Integration between different processes [21, 22] of counteracting the loss of organisation continuity is particularly important for the sake of creation of effectively operating system. It will be covered by statutory competence of management of a particular organisation. Such operations and actions will be based upon legal regulations and organisational and administrative procedures as well as available human, information, material and equipment resources for different departments of executive system (rescue, fire, evacuation, transport and similar units and departments). Procedures for various processes implementation will constitute one of significant elements of targeted crisis response system, including proper ways of monitoring and identifying threats, counteracting those threats, which may be predicted and prevented (e.g. breaking into computer system and the like) and ways of responding – adequate for the nature of a particular threat as well as rules for elimination of negative effects and rules for cooperation with external entities with the use of threats notification systems. The above-said procedures should have an individual character. It means, that their level of detail must be sufficient for a particular decisive level [6]. Specific action features should be approached in a uniform manner with emphasizing the scope of operations and indication of who, where

[5] Distinction between those terms is presented in: K. Bolesta-Kukułka, *Decyzje menedżerskie*, PWE, Warszawa 2003, p. 190-194.

[6] J.A.F. Stoner, R.E. Freeman, D.R. Gilbert jr, *Kierowanie*, PWE, Warszawa 1997, p. 239.

[7] A. Białas, *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie*, WN-T, Warszawa 2007, p. 182.

and when should use, and who and when should supervise and accept the manner of implementing particular activities together with the scope of their monitoring.

An issue of information safety threatening is important for different entities and public authorities. Protection of interests and safety of citizens and of the whole society is a statutory duty to be performed by public authorities of every country and every entity/organisation. Taking into consideration safety of information resources its status should be that of "non-threatened, safe and certain"[8]. Therefore, crisis situations and threats should be perceived on one hand as resulting from the operation of forces of nature (real occurrence of natural disasters and natural catastrophes), and on the other hand as threats resulting from irresponsible human activity. The manner and possibility of counteracting in each of those cases may differ significantly even on the grounds of the level of potential and real risk occurrence. Projects related to safety ensuring should have rather a preventive character and should consist in recognising, detecting and preventing situations that may cause threats [11]. Technological development enables us not only to predict threats but also to reduce their negative effects. It concerns in particular potential threats resulting from technical failures in relation to the results of loss of information continuity.

On the basis of ISO 9000 standard [18, 19] one can ascertain that safety assurance procedure, as well as information continuity may be specified as agreed upon manner of conducting activity or process guaranteeing special safety level [14, 16] of information resources. Procedure is in the form of document, which specifies targets, defines responsibility and indicates the chronological order of executing particular actions. It may be illustrated in the form of a system, where the process targets are emphasized as well as threats, safety indicators and necessary input resources as well as result of action and description of the very process and authorisations together with specification of scope of responsibility. Procedures are usually part of planistic documents, which relate safety policy to detailed/routine projects and involve mainly threats avoiding (including reduction of subjective factors) or effective operation in case of crisis situation (actual occurrence of selected threats). Safety procedures are being prepared in particular for the operating unit. As mentioned before every procedure should be adapted to universal model of contents (see Table No.1).

In order to ensure activity consistent with the relevant procedure all projects should be presented in such a manner that would directly influence clarity of projects covered by the procedure. Analysis[9] of safety assurance and maintaining information

[8] *Słownik języka polskiego PWN*, vol. 1, Warszawa 1978, p. 147.

[9] For instance analysis of event which took place in September 11, 2001 in New York (M. Gallagher) shows the problem of shortcomings in continuity plans (broad range of disasters has not been taken into account but in fact only single events). Furthermore, action plans (procedures) were too detailed and ineffective and plans were difficult to obtain and outdated. Actions were too optimistic and temporarily planned and action plans often have not even been tested, it constituted a significant

continuity of every organisation allows for undertaking reasonable actions prior to the crisis (preventing crisis situation) as well as after an undesirable event occurrence. Attention should be paid to the fact that procedures and plans of continuity require systemic approach to the matter of safety assurance to the organisation by means of creation of integrated set of procedures. Development of multi-optional procedures including various threats and corresponding organisational situations requires prior preparation of procedures for preventive activities, activated in case of crisis situations and eliminating effects under real time and resource constraints. Continuous threats analysis and adequate procedures updating are of significant importance. The matter of organisational procedures prepared for the sake of information safety of the organisation and effective response in case of threatening situation and crisis situation always requires further formalization and unification. Moreover, procedures and systems of safety assurance should be perceived in terms of counteracting acts of cyber terrorism. One of the methods for increasing effectiveness of information continuity procedure in case of crisis management system is the use of infrastructure and services available under the "cloud" computing.

Table No. 1. Universal model of elements of crisis response procedures (safety)

No.	Operation
1.	Specifying name of entity that the procedure concerns and organisational unit as well as location of its storage.
2.	Name of the procedure, specification of used terms (short definitions) and specification of number of pages where it has been described with place for annotations concerning its updating.
3.	Date of elaboration, data concerning an author and accepting entity as well as approving entity
4.	Specifying purpose of the procedure and the scope of its operation as well as indicating expected results.
5.	Indicating major contractors and specifying persons (functions) responsible for operations covered by the procedure
6.	Specifying manner of acting in a given case that the procedure concerns. It may be illustrated in the form of algorithm presenting the order of undertaken actions. Oral presentation may be accompanied by a diagram. It may be also presented in the form of legible graphic demonstration.
7.	Specifying cooperating entities (internal and external) as well as indispensable physical resources and manner of communication with indicating necessary technical means of communication

negligence, moreover, some organisations did not indicate alternative area for dislocation that would allow for continuity of functioning in case of threatening situation.

No.	Operation
8.	Indicating major threats that may be encountered during implementation of procedure and the manner of making records (documentation of implemented projects).
9.	Indicating documents of a higher rank constituting the legal basis for the developed procedure.
10.	List of attachments.

The source: Personal elaboration on the basis of Falco, Joe, et al.: *IT Security for Industrial Control Systems*, NIST IR 6859, 2003, http://www.isd.mel.nist.gov/documents/falco/ITSecurityProcess.pdf.

4. "Cloud" computing as a multi-level service

"Cloud" computing is a set of different IT services provided in virtual cyberspace [24, 25, 26]. It creates favourable conditions for the development and functioning of different types of organisations – especially with limited potential or in special cases – through the use of widely available ICT infrastructure and available information resources. Both public authorities as well as other organisations important for the national defence and security - may use those services provided by external organisations. The above mentioned services may include not only access to ICT infrastructure adapted to the needs of a user but also provide access to selected applications. "Cloud" computing [3, 27, 28] is related to virtualisation of information services in compliance with relevant principles, like:

a) virtualisation of information resources allowing for their dislocation
b) providing access to dedicated resources for every registered user including flexible scaling system and meeting the particular needs of a given organisation (nominated post holder)
c) automatic creation of new virtual resources as well as deleting the existing ones.

It is important to note that fees for particular services provision will be charged only for actually used resources. "Cloud" computing is the result of a long-term process beginning with the use of computers with great amount of computing power of the mainframe type by the so called subscribers using remote dedicated resources. First network solutions created the possibility for both individual as well as group users to freely operate in local and wide area networks. Network infrastructure [29] allows for virtualisation of an organisation and "flattening" of its organisational structures by means of free access provision to different information resources (with restricted access rights) regardless of its place in organisational structure.

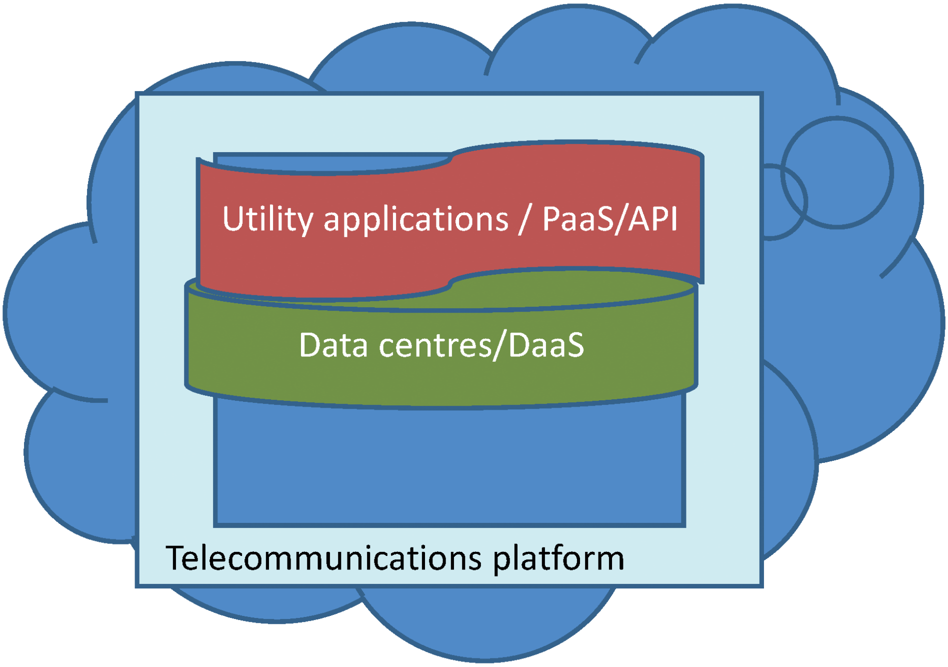

Fig. 2. Service levels available in "cloud" computing[10]

"Cloud" computing becomes an attractive offer of modern services, which strengthen the potential of every organisation (Fig. 2) taking into account its different levels[11] , which specify the scope of such service by means of:

a) providing access only to technical infrastructure (the so called IaaS for instance the Amazon platform),

b) making use of selected, dedicated applications (the so called PaaS, that is IaaS + applications for instance the Microsoft),

c) maintaining and providing access to data centres (the so called DaaS , that is PaaS + data resources),

d) maintaining and providing access to tools for creation of individual applications (the so called API, that is DaaS + PaaS).

The above mentioned service levels specify their character beginning with provision of short-term access to technical infrastructure resources and creation

[10] Personal elaboration on the basis of: A. Mateos, J. Rosenberg, *Chmura obliczeniowa. Rozwiązania dla biznesu*, Wyd. Helion, Gliwice 2011.

[11] ut1} Iaas (Infrastructure as a Service), Paas (Platform as a Service), SaaS (Software as a Service), CaaS (Communications as a Service), DaaS (Data as a Service), API (Application Programming Interface).

of individual applications as well as the use of standard applications. Taking into account the ICT infrastructure as an essential component of critical infrastructure – one can say that in case of crisis management systems it will mean not only improvement of the ICT environment, but most of all increase of the level of information continuity. As far as organisational aspect is concerned, it is possible to provide access to selected resources from any place in the network of the Internet type or from corporate networks according to the expected security level. Moreover, it should be emphasized as well that significant costs reduction is clearly visible here, meeting the scalability criterion and integrating different solutions and individual data resources[12], as well as resources of selected co-producers of particular processes under crisis response system. Even rough analysis of "cloud" computing properties indicates a possibility of reducing expensive IT investments due to access to ICT infrastructure and related services according to actual value of dynamically scalable service meeting the organisation requirements. It seems that both big organisations as well as structures of public administration may be cloud computing beneficiaries. With the use of cloud computing services they may quickly response to any changes in the environment (crisis situations, threats) according to the scalable demand[13]. Especially decisions delays described in chapter 3 can be managed by using cloud computing services. Each stakeholder can either read or alter information from any device (pace of receiving information) as well as from any place (e.g. in the place where crisis happened).

5. Framework concept of ensuring information continuity of crisis management systems in the aspect of using services in cloud computing

Providing authorised entities, acting in geographic dispersion, with access to IT resources is a challenge that modern organisations of 21st century have to face. Obviously, in case of crisis management systems, in particular in case of crisis response systems, process structures should be preferable as a flexible solution. It is required by dynamically changing situation [21, 22]. Process architecture emphasizes equality of cooperating entities and is oriented on quality of purpose carried out in its entirety with successive verification of information continuity criterion.

[12] A possibility of off-line edition with intelligent synchronization of changes introduced in online mode constitutes an important element in this area. Moreover, there is neither need to update the Microsoft Office suite nor to implement relevant software, like the SharePoint®. Generally speaking, it is possible to edit Office files with easy sharing, files versioning and with no need to create backup copies.

[13] Another significant element, as far as IT resources are concerned, is the possibility of implementing the so called go-to-market strategy without geographical and investment restrictions.

The CC class services[14] enabling access to information of different resource types dispersed territorially, without clear time restrictions – constitute the actual challenge for the modern crisis management systems. Critical infrastructure, including individual ICT potential of every organisation, is limited to a significant extent. User/recipient – oriented IT services require access to reliable, integrated and duly verified private information resources and information resources owned by other entities. The use of proper information technologies, enabling coordination of mutual projects implementation in specified period of time becomes a strategic purpose.

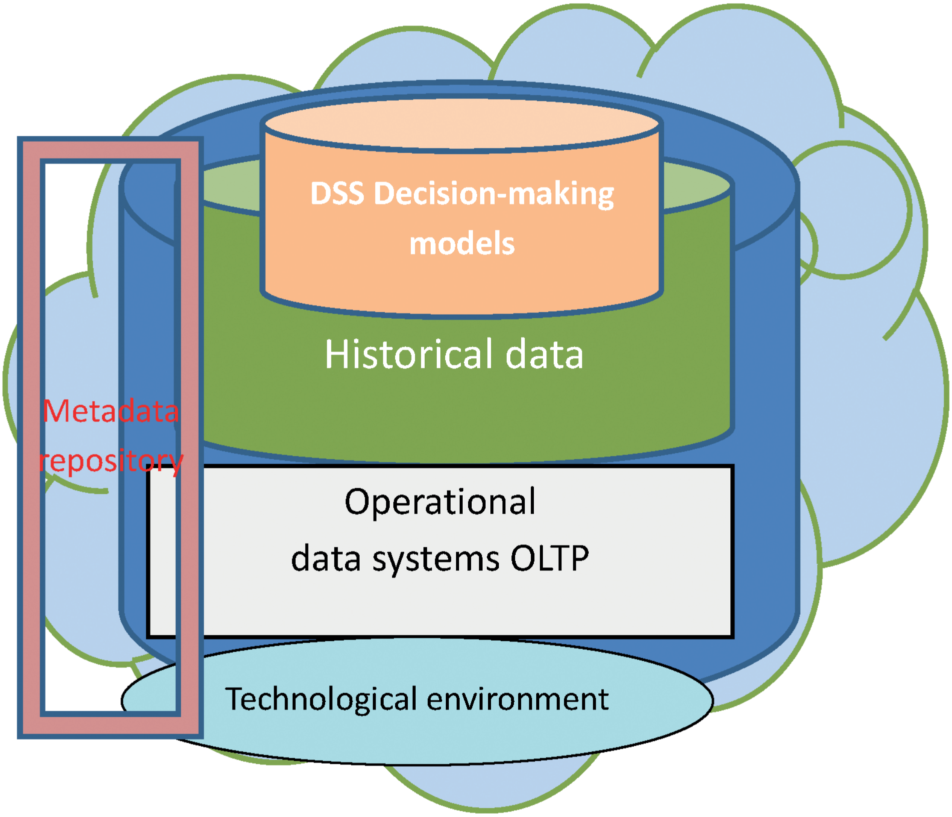
DSS Decision-making models
Historical data
Metadata repository
Operational data systems OLTP
Technological environment

Fig. 3. Integration of information resources with the use of CC class services (personal elaboration)

Modern management and crisis response systems[15] should emphasize elimination of information barriers [12]. The CC class services enable an on-line response

[14] Available in „cloud" computing.

[15] S. Kliciński, *Problemy implementacji podejścia procesowego*, ISBN 978-83-7011-969-0. Wyd. UE, Wrocław 2009, p. 58.

and allow for exploration of environment resources in case of shortcomings in personal potential. Those services may enable integration of decisions and actions with decentralised decision-making process. Inclusion of relevant security mechanisms provides every entity with certain guarantee of maintaining expected level of information continuity[16]. Moreover, a possibility of participating in global (multi-entity) process, which enables the maintenance of operations integrity with decentralised decision-making process is also worth mentioning. Both OLTP[17] as well as OLAP[18] class systems (Fig. 3) become the basis for changes of contemporary organisations as entities operating under crisis situations. As a result of "horizontal" cooperation between processes and striving to reduce the risk of loss of information continuity competence and decision-making transparency is required. Integrated IT management systems are the tools that require information and decision-making arrangement (meta-data repository) in different areas of decision-making process[19].

Tools and OLTP and OLAP class IT systems [1, 2] ensure continuity and effectiveness of functioning, conditional upon access to updated information on personal and cooperating entities' capabilities. Due to such solutions a strong reorientation to implementation of common tasks and the use of dispersed resources with possibility of ongoing monitoring and control of time, resources condition, costs and effects of operation is possible. Communication improvement as well as cooperation with the use of tools of "workflow" type in network model are meaningful as well.

OLTP class systems are not sufficient therefore it is important to search for certain models of functioning. BI class systems[20] constitute important system supplementations, which may generate not only long-term evaluations, but also support knowledge discovery. Collected historical data after proper arrangement enable a possibility to conduct multi-sectional analysis according to any criteria (attributes/dimensions, including time, place, object and subject of operations and the like), which may mean multidimensional evaluation including strong timely requirements and predicted situation in the future with the use of proper tools[21]). Those systems ensure dynamic model of functioning of organisation due to access to IT resources[22] on-line (with the use of CC services) in proper time and place or according to settled schedule in the sphere of monitoring of the state of the use of

[16] Information continuity is a component of system continuity within the meaning of material, energetic and similar continuity of implementation of processes under dynamically changing conditions.

[17] On-Line – Transaction – Processing (on-line IT systems).

[18] On-Line – Analytical – Processing (IT, analytical systems supporting analysis and data mining the so called DM).

[19] DSS (Decision Support Systems).

[20] Business Intelligence, that is „providing the right information to the right person at the right time". Dashboards

[21] Dashboards.

[22] Vide big data and future-predicting algorithms.

particular processes and reporting the occurrence of emergency situations[23]. The use of such models is conditional upon clear map[24] of major (basic) processes of strategic importance, as well as auxiliary (supporting), which are complementary to the major processes.

Process strategy aims at ensuring continuity in implementation of particular processes with complete identification of map of every process including the time and the scope of operations of particular co-producers with their mutual trust. Participation of different entities/contractors/subcontractors requires access to updated information in order to reduce costs of business operations and improve effectiveness [8]. Effective operations under such conditions require collecting data in database and data warehouse. Process organisation implemented under the "cloud" computing emphasizes a possibility of cooperation between different entities dispersed locally and globally[25].

Effectiveness of crisis response processes is related to value added for every "participant" according to his competence and experience as well as value of information resources located in the "cloud". Personal information resources as well as professional exposure in the Internet are of significant importance to the creation of personal level of information security as well as functioning continuity, as well as quick resumption of information on environment, influencing effective functioning in territorially unrestricted area for instance proposals on WWW on the basis of the contents of OLTP and OLAP class systems of particular processes[26] Systems available under CC services using mechanisms of data mining[27] may constitute effectiveness increase platform for contemporary organisations.

6. Conclusion

CC services allow for creation of secure organisations. It is very important for the sake of virtualisation of actions and integration of different processes directly conditional upon access to information resources. CC class services eliminate access barriers. It is possible to use external services in case of the crisis management systems. New perspectives appear both in the sphere of autonomic organisations as well as those, which enter into alliances with the environment. Uniform and unambiguous/updated information resources reflecting operations of different dispersed entities, but joined

[23] portal BI.pl

[24] Strategia X-engineeringu.

[25] T. Kopczyński, *Outsourcing w zarządzaniu przedsiębiorstwami*, PWE, Warszawa 2010, s. 116.

[26] J.J. Lambin, *Strategiczne zarządzanie marketingowe*, PWN, Warszawa 2001, p. 304.

[27] One of the means for analysis and presentation concerning data collected in the "cloud" computing may be a cluster analysis consisting in examination of data distribution according to the location criteria. The process coordinator may go deep into the analysis of causes. Such tools become of strategic importance as far as information effectiveness is concerned.

by common purpose/process, may become the source of improvement. IT systems available under CC (OLTP, OLAP, DM) may be the basis for effective operation and decision-making activity in the crisis management and crisis response systems. It is important to bear in mind an integration of different process classes perceived as systems providing support under internal and external relations. CC services strengthen the potential of organisation and may influence an increase of information continuity.

LITERATURA:

1. A. Januszewski, *Funkcjonalność informatycznych systemów zarządzania. Systemy Business Intelligence*, T. 2, Wydawnictwo Naukowe PWN, ISBN: 978-83-01-15599-5, Warszawa 2008, p. 384/p. 250.
2. D.T. Larose, *Metody i modele eksploracji danych*, Wydawnictwo Naukowe PWN, ISBN 978-83-01-15467-7, Warszawa 2008, p. 240.
3. A. Mateos, J. Rosenberg, *Chmura obliczeniowa. Rozwiązania dla biznesu*, Wyd. Helion, ISBN 978-83-246-3416-3, Gliwice 2011, p. 276.
4. BS 25999-1: 2006: *Business continuity management. Code of practice.*
5. BS 25999-2: 2007: *Specification for business continuity management.*
6. K. Ficoń, *Inżynieria zarządzania kryzysowego. Podejście systemowe*, Wyd. Bel Studio, Warszawa 2007, p.
7. GAO-04-354, *Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems*, U.S. GAO, 2004, http://www.gao.gov/new.items/d04354.pdf.
8. W. Kitler, *Istota zarządzania kryzysowego*, [w:] *System reagowania kryzysowego*, pod red. J. Gryza i W. Kitlera, Wyd. Adam Marszałek, Toruń 2007.
9. COMMITTEE OF THE EUROPEAN COMISSION, Brussels, dated 12.12.2006 KOM(2006) 786 final version: Communication from the Commission on the European Programme for the Critical Infrastructure Protection.
10. J. Łagowski, *Disaster: Backup & Recovery – copy made by DR in: IX PLOUG Conference materials*, Kościelisko, October 2003.
11. K. Liderman, *Model planów ciągłości działania według typów zagrożeń dla wybranych klas organizacji,* Elaborationmadeunder the task 5.1. of the research project PBZ--MNiSW-DBO 01/1/2007.
12. W. Miszalski (co-author): *An Evolution of Security Environment and Armament Development Planning*, (IOZ) Warszawa 2011, pp: 263-286, ISBN/ISSN: 2082-2677.
13. NERC BACKUP CONTROL CENTER. A Reference Document EPRI Project RP2473-68. W: NERC Operating Manual. March. 2008.
14. NFPA 1600: *Standard on Disaster/Emergency Management and Business Continuity Programs. 2007 Edition.*
15. NISCC *Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks*, National Infrastructure Security Coordination Centre, London, 2005, http://www.cpni.gov.uk/docs/re-20050223-00157.pdf.

16. NIST Special Publication 800-34: *Contingency Planning Guide for Information Technology Systems. June. 2002.*
17. NIST Special Publication 800-82 (SECOND PUBLIC DRAFT): *Guide to Industrial Control Systems (ICS) Security*. September 2007.
18. PN-ISO/IEC 15408-1:2002: *Technika informatyczna – Techniki zabezpieczeń – Kryteria oceny zabezpieczeń informatycznych – Część 1: Wprowadzenie i model ogólny*.
19. PN-ISO/IEC-17799:2005 *Technika informatyczna – Praktyczne zasady zarządzania bezpieczeństwem informacji.*
20. P. Zaskórski (red.) *Zarządzanie organizacją w warunkach ryzyka utraty informacyjnej ciągłości działania*, Wyd. WAT, ISBN 978-83-62954-04-9, Warszawa 2011, p. 229.
21. P. Zaskórski, A. Suszek, *Zarządzanie procesami projektowo-wdrożeniowymi systemów bezpieczeństwa*, V International Conference on Security, Crisis management, Gdynia 2007.
22. P. Zaskórski, *Koncepcja informatyzacji systemu reagowania kryzysowego MON*, AON, Warszawa 2002.
23. P. Zaskórski, W. Zaskórski, *Hurtownie danych w systemach logistycznych. (Data storehouse under logistic management systems)*, XII Scientific Conference *Automation of command*, Gdynia 2004, s. 16/8.
24. W. Zaskórski, P. Zaskórski, *Strategia benchmarkingu w kreowaniu infrastruktury teleinformatycznej systemów dowodzenia SZ RP i zarządzania kryzysowego* (przyjęte do druku Wyd. Bellona, Warszawa 2014).
25. D. Pałka, W. Zaskórski, P. Zaskórski, *Cloudcomputing jako środowisko integracji usług informatycznych*, http://zeszyty-naukowe.wwsi.edu.pl/zeszyty/zeszyt9/Cloud_computing_jako_srodowisko_integracji_uslug_informatycznych.pdf
26. M. Kuźniar, *Chmura obliczeniowa w służbie administracji*: https://kb.oktawave.com/Knowledgebase/Article/GetAttachment/179/424
27. M. Northend, *7 powodów, dla których warto wybrać komunikację w chmurze*, http://inwestycje.pl/it_ebiznes/7-powodow-dla-ktorych-warto-wybrac-komunikacje-w-chmurze;176151;0.html
28. H. Young, *Cloud Computing for the Public Sector*, http://rley.org/doku.php?id=work:cloud_computing_for_the_public_sector
29. B. Kowalczyk, *Sieci i usługi telekomunikacyjne w zarządzaniu kryzysowym*, http://yadda.icm.edu.pl/yadda/element/bwmeta1.element.baztech-article-BATA-0013-0032/c/httpwww_itl_waw_plczasopismatiti20111-264.pdf.

WYBRANE PROBLEMY KONTYNUACJI INFORMACYJNEJ SYSTEMU ZARZĄDZANIA KRYZYSOWEGO W ZWIĄZKU Z UŻYCIEM KOMPUTEROWEJ CHMURY

Streszczenie: Usługi CC są aktualną propozycją dla wirtualizacji działań, a jednocześnie integracji różnych procesów bezpośrednio warunkowanych dostępem do zasobów informacyjnych. Usługi klasy CC mogą eliminować barierę dostępu oraz umożliwiać wykorzystanie zasobów informacyjnych w relacjach wewnętrznych i zewnętrznych dla systemów zarządzania i reagowania kryzysowego. Usługi CC mogą istotnie wzmocnić potencjał organizacji, a także sprzyjać wzrostowi informacyjnej ciągłości działania poprzez wykorzystanie wielu sprawdzonych, zaawansowanych aplikacji.

Słowa kluczowe: ciągłość działania, informacyjna ciągłość działania, systemy zarządzania kryzysowego, chmura obliczeniowa, sytuacja kryzysowa/kryzys, bezpieczeństwo informacyjne, wirtualizacja zasobów, usługi w chmurze