EKONOMSKA ISTRAŽIVANJA-ECONOMIC RESERACH
ISSN 1331-677X print

2013 Volume 26 (1): 183-202

IMPLEMENTATION OF IT GOVERNANCE STANDARDS AND BUSINESS CONTINUITY MANAGEMENT IN TRANSITION ECONOMIES: THE CASE OF BANKING SECTOR IN CROATIA AND BOSNIA-HERZEGOVINA

Mario Spremić [a], Nijaz Bajgorić [b], Lejla Turulja [c]

[a] Full Professor, Ph.D, University of Zagreb, Faculty of Economics & Business Zagreb, Department of Information Systems, Trg J. F. Kennedy-a 6, 10000 Zagreb, Croatia, mspremic@efzg.hr
[b] Full Professor, Ph.D, University of Sarajevo, School of Economics and Business Sarajevo, Trg oslobođenja – Alija Izetbegović 1, Sarajevo, Bosnia and Herzegovina, nijaz.bajgoric@efsa.unsa.ba
[c] Senior Teaching Assistant, MSc, University of Sarajevo, School of Economics and Business Sarajevo, Trg oslobođenja – Alija Izetbegović 1, Sarajevo, Bosnia and Herzegovina, lejla.turulja@efsa.unsa.ba

ARTICLE INFO

Article data:
- Received: 4 February 2012
- Accepted: 8 July 2012

JEL classification:

Keywords:
- Business continuity management
- IT governance
- IT risk
- IT audit
- Downtime

ABSTRACT

Over the past decade business continuity management (BCM) has been treated mainly from either technology or planning perspective. This paper goes a step further and considers BCM from the IT governance view. In addition, the standards and legislation activities that help in that sense are evaluated. Implementation of industry best practices standards and processes such as ITIL and CobiT combined with other IT-related solutions can deliver substantial risk reduction and reduce business risks and result with reduced system downtime. The cases of the implementations of main information technology (IT) standards in the banking sector of Croatia and Bosnia-Herzegovina from those two perspectives are explored.

Reference to this paper should be made as follows: Spremić, M., ; Bajgorić, N.; Turulja, L. 2012. Implementation of IT governance standards and business continuity management in transition economies: The case of banking sector in Croatia and Bosnia-Herzegovina, *Ekonomska istraživanja – Economic Research 26(1): 183-202.*

I. INTRODUCTION

Recently, with advances in Internet technologies and e-business, the need for achieving "a near 100%" level of application availability was brought up yet again. Consequently, the term of "business continuity management (BCM)" was coined up and became a significant part of organizational information management. Most of today's businesses are under pressure to keep their information systems (IS) running on "24/7/365" basis and ensure data and applications' continuous availability. Business continuity (BC) strategy has become No1 item for both CEO's and CIO's priority lists. According to the Forrester Report (2009), almost 80% of respondents reported that their firms have had to provide proof of BC readiness. Fast, continuous, reliable data access and data availability, are just a few of the objectives of contemporary business.

Business continuity, business continuance, business resilience, high availability, fault/disaster tolerance, is just a few of the terms that are used in modern business. Business continuity today relies on continuous computing technologies that are aimed at providing an efficient operating environment for "always-on" computing which is in turn technological prerequisite for "always-on" business. Simply put, implementation of continuous computing technologies provides a platform for "keeping business in business" as business-critical applications are installed on enterprise servers; these servers are run by server operating systems, with all of them backed-up by data storage systems and supported by several fault-tolerant and disaster-tolerant technologies.

Today's business is simply bound to its information system (IS) and dependent on information technology (IT). In addition to standard business risks, the dependence on IT platforms produces the IT-based business risks as well. Identifying the IT-related threats has become an important part of managing information resources in an organization. Moreover, it has to be considered as a threat that may cause problems to a business just like any other threat (physical, natural, commercial, competition). Businesses apply several approaches in order to avoid (reduce, mitigate, manage) the IT-related risks and other business risks. There exist several standards and recommendations that specify the desired methods for managing information resources. In addition to standards prescribed by international standardization agencies, various national standards and recommendations and best practices of various private companies are used.

The objective of this paper is to reveal how IT governance standards can be implemented in general and in the banking sector in SEE countries within the framework of business continuity management. This research includes cases from banking sector in two SEE countries: Croatia and Bosnia-Herzegovina (BandH). However, the research framework and lessons learned may provide some ground for the generalization of this research topic for other countries, those in the SEE region and in general.

II. LITERATURE REVIEW AND RESEARCH MODEL

Business continuity management as a separate IT-discipline emerged 15 years ago. Business continuity has been treated as both IT and managerial issue particularly after the e-business boom and the "9/11" event. Business continuity is achieved by implementing continuous computing IT platforms having high availability ratios.

According to IDC (2006), high availability systems are defined as having 99% or more uptime. IDC defined a set of different availability scenarios according to availability ratio, annual downtime, user tolerance to downtime with regard to several continuous computing technologies that are available today:

TABLE 1 - IDC CLASSIFICATION OF AVAILABILITY SCENARIOS

	Availability	Average Annual Downtime	User Tolerance to Downtime
Fault Tolerant	99,999%	5 minutes	None
Continuous Availability			
Cluster	99,9%	8 hours	Business Interruption
High Availability		45 minutes	Lost Transaction
Stand-alone GP or	99,5%	43 hours	Tomorrow is Okay
Blade Server w/RAID		23 minutes	

Source: Adapted from IDC, 2006

Business continuity institute (http://www.thebci.org) defined business continuity management as a holistic management process that identifies potential impacts that threaten an organization and provides a framework for building resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation and value creating activities. Its primary objective is to allow the executives to continue to manage their business under adverse conditions, by the introduction of appropriate resilience strategies, recovery objectives, business continuity and crisis management plans in collaboration with, or as a key component of, an integrated risk management initiative.

Recent research papers on BCM focus either on frameworks or separate technologies that are used in order to improve the availability levels. Vatanasombut et al. (2008) argue that the proliferation of Internet has not only allowed businesses to offer their products and services through Web-based applications, but it has also undermined their ability to retain their customers. Lump et al. (2008) provide an overview of the state-of-the-art architectures for continuous availability concepts as high-availability (HA) clustering on distributed platforms and on the mainframe. They present aspects of service management, including the use and orchestration of process-based (ITIL) systems management tasks within disaster recovery (DR) scenarios. Melton and Trahan (2009) argue that critical risks demand critical attention. Hiles (2004) estimated that IS downtime puts direct losses on brokerage operations at $4.5 million per hour, banking industry $2.1 million per hour, e-commerce operations $113.000. Botha and Von Solms (2004) proposed a cyclic approach to business continuity planning. Gibb and Buchanan (2006) defined a framework for the design, implementation and monitoring of a business continuity management program within the context of an information strategy. Pitt and Goyal (2004) see BCM as a tool for facilities management. Walker (2006) considers outsourcing options for business continuity. King (2003) introduced a term of "Business Continuity Culture" and underscored the fact that "If you fail to plan, you will be planning to fail". Williamson (2007) found that in business continuity planning, financial organizations are ahead of other types of businesses. Bertrand (2005) researches the relationships between business continuity and mission-critical applications. Gerber and Solms (2005) emphasize the need for a holistic approach that should include a carefully planned security policy, the use of technology and well-trained staff. Finch (2004) revealed that large companies' exposure to risk increased by inter-organisational networking and that having small and medium enterprises (SMEs) as partners in the supply chain management (SCM) further increased the risk exposure.

Kuhn and Sutton (2010) explored the alternative architectures for continuous auditing by focusing on identifying the strengths and weaknesses of each architectural form of enterprise resource planning (ERP) implementation. Kadlec (2010) reports on the IT DR planning practices

of 154 banks in the United States. Arduini and Morabito (2010) argue that the financial sector sees business continuity not only as a technical or risk management issue, but as a driver towards any discussion on mergers and acquisitions. Spremic (2008, 2009) argued about the role of IT governance concept, especially in applying the IT risk management procedures at executive levels. As the organizations are becoming increasingly dependent upon IT in order to achieve their corporate objectives and meet their business needs, the necessity for implementing widely applicable IT governance best practices standards and methodologies, offering high quality services is evident. The issue of managing the IT risks becomes less and less a technical problem, and more and more the problem of the whole organization that is a 'business problem' and many companies nowadays formally nominate executive directors for such activities. Therefore, it is highly recommendable that BC strategy becomes a part of IT governance procedures and that companies have a BC manager that is outside the IT department. DeHaes and Grembergen (2009) suggest that there is a clear relationship between the use of IT governance practices and better business/IT alignment.

All these works deal with BCM either from managerial or organizational perspective. However, they lack some guidelines for a comprehensive approach in implementing numerous so-called continuous computing technologies and IT-standards and compliance regulations that can provide an integrated platform for business continuity. Business continuity management consists of strategies, policies, activities and measures that business undertakes in order to survive when some sort of catastrophic event occurs. Even though it represents a managerial activity, at the end, business continuity in information age relies on high-ratios of application/data availability, reliability and scalability that should be provided by server operating environment. A systemic model used in this paper is given in Figure 1.

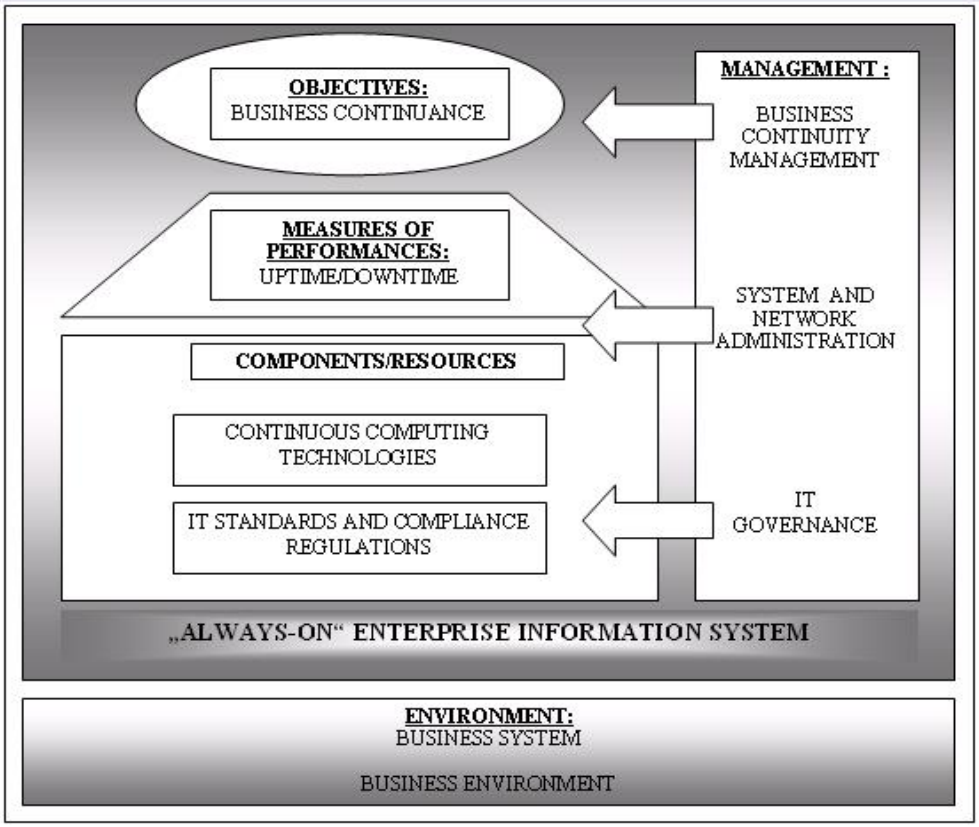

FIGURE 1. SYSTEMIC MODEL OF BUSINESS CONTINUITY AND IT GOVERNANCE
Source: Authors

The model is based on Churchman's systems approach (1968) which defines the system by using the following five dimensions: i) Objectives and measures of performances, ii) environment, iii) resources, iv) components, v) management. It considers the relations between IT governance standards and business continuity within the concept of continuous computing technologies that can be applied in order to enhance applications' availability ratios and hence the whole business continuance. The implementation of these standards in banking sector of two SEE countries (Croatia and Bosnia-Herzegovina) is considered as a case.

As can be seen from this figure, IT governance is considered as part of management dimension of the Churchman's systemic model, together with business continuity management and system administration. In most cases, implementation of the IT standards and compliance regulations is done by forcing organizations to implement several continuous computing technologies such as remote backup, recovery, mirroring. This model is further explained in section 6.

III. BUSINESS CONTINUITY MANAGEMENT AND IT GOVERNANCE

The IT governance relates to IT practices of boards and senior managers. The question is whether IT structures, processes, mechanisms and IT decisions are made in the interest of shareholders and other stakeholders, or primarily in the executives' interests. IT governance closely relates to

corporate governance, the structure of the IT organization and its objectives and alignment to the business objectives. The primary focus of IT governance is on the responsibility of the board and executive management to control formulation and the implementation of IT strategy, to ensure the alignment of IT and business, to identify metrics for measuring business value of IT and to manage IT risks in an effective way (Spremic, 2009). IT governance is the process for controlling an organization's IT resources, including information and communication systems and technology (Hunton, 2004). It is an integral part of enterprise governance and consists of the leadership and organizational structures and processes that ensure that the organization's IT sustains and extends the organization's strategies and objectives. Van Grembergen (2005) defined IT governance as the organizational capacity exercised by the Board, executive management and IT management to control the formulation and implementation of IT strategy and in this way ensure the fusion of business and IT.

A good, or rather, inevitable approach for managing IT risks includes thorough audit and quality assessment of all aspects of IS and IT, including hardware, software, data, networks, organization and key business processes. The primary goal of the information system audit (IT/IS audit) is to identify the key business processes that depend on IT, to systematically and carefully examine their IT control efficiency, to identify key risk areas and constantly measure the risk level, to warn about possible failures, as well as to offer suggestions to the executive management how to improve current IT risk management practices (Spremic et al, 2008).

A. Possible strategies for BC risk responses

Once the organization has identified, classified and assessed IT risks, risk owners and 'affected' process owners are to be identified, appropriate responses should be developed and specific cost-effective controls over those risks should be designed. Responses to BC risk may include following strategies:

- Acceptance – the organization chooses to live with the risk and to constantly monitor its level (gravity and impact on the business and business processes),
- Reduction – the organization takes steps to reduce the impact (gravity) or the probability of the risk occurrence,
- Avoidance – the organization chooses to fully or partially avoid the risk,
- Sharing – the organization transfers the risk by, for example, purchasing insurance, outsourcing risk management services, or engaging in partnership(s) regarding the risk management process to fully or partly cover risk exposure (especially in business continuity and disaster recovery plans).

Strategies for IT risks responses usually mean that specific IT controls need to be implemented and their efficiency constantly monitored. Control activities are the policies, procedures and practices that are put into place so that business objectives are achieved and risk mitigation strategies are carried out. Control activities are developed to specifically address each control objective to mitigate the risks identified. An IT control objective is a statement of the desired result or purpose to be achieved by implementing control procedures in a particular IT activity. The IS audit activities usually include the examination of the IT control efficiency. When doing so, IS auditors commonly perform test of IT controls using specific metrics (for example, RTO, RPO for business continuity process) and maturity models. Common metrics for testing the efficiency of business continuity plan can be:

- MTBF (mean time between failures) represents an important system characteristic, which help to quantify the suitability of a system for a potential application. MTBF is the measure

of the systems' functionality and service level. MTBF is often connected to the mean time to repair (MTTR).

- Availability represents the percentage of time when system is operational (for example, 99% availability is meant that the system downtime is 3,65 days per year, while 99,99% availability rate means that the downtime is 52 minutes per year).
- First fix rate - measures the percentage of incidents that successfully restored on the first fox attempt. It is leading indicator of system availability and MTTR.
- RTO (recovery time objective) - the period of time within which systems, services, applications or functions must be recovered after an outage. It is maximum tolerable length of time that an IT infrastructure can be down after a failure or disaster occurs.
- RPO (recovery point objective) – the maximum amount of data loss an organization can sustain during an event. It is also the point in time (prior to outage) in which systems and data must be restored to.

B. IT governance methodologies and frameworks that supports BCM

All kinds of risks that are related to information technologies and their potential threats to business should be a part of an integrated risk management on organizational level. Risk management is an ongoing process designed to assess the likelihood of an adverse event occurring, implement measures to reduce the risk that such an event will occur and ensure the organization can respond in such a ways to minimize the consequences of the event.

Today's business is constantly under a pressure not only from customers, suppliers and competitors but from regulatory requirements as well. Implementing IT governance and IS audit frameworks may help organizations manage IT risk level, especially BC risks. Various groups have developed world-wide known IT governance guidelines, standards and regulations that specify the best methods for managing IT functions of a company. In addition to standards prescribed by international standardization agencies, various national standards and recommendations and best practices of various companies are used. These standards and frameworks are:

- COBIT (control objectives for information and related technology) issued by ISACA (information systems audit and control association) created as a framework for establishing control of the relationship of IT processes and business requirements and represent basic IT governance framework.
- ITIL (information technology infrastructure library) is a collection of best-practice solutions achieved in practice of managing IT services issued by the British Office of Government Commerce.
- NFPA 1600 (www.nfpa.org). NFPA 1600 is the Standard on Disaster/Emergency Management and Business Continuity Programs, was prepared by the Technical Committee on Emergency Management and Business Continuity.
- ISO/IEC 27000:2005 (The Code of Practice for Information Security Management) – the series of international standards (ISO 27000 – ISO 27008) associated with managing information security.
- ISO/IEC TR 1335 (Guidelines for the Management of IT Security) is a technical document that includes information and instructions on IT security, both from management aspect and from implementation aspect.
- ISO/IEC 15408 (Security Techniques—Evaluation Criteria for IT Security) is used as reference for review and certification of IT products and services.

- Risk management standard (IRM) as a result of the efforts made by the major risk management associations in the UK including the IRM, AIRMIC and ALARM.
- TickIt was issued by the British standards institute and is use for review and certification of software quality management systems.
- COSO internal control—integrated framework was issued by COSO and includes a framework whose application will improve the process of financial reporting through improved internal control processes.
- BS 25999 business continuity standard, BS 25777 information and communication technology standard.

According to IDC's White Paper (2009), by adopting industry best practices (for example ITIL, CobiT) and updating IT infrastructure, companies can lower annual downtime by up to 85%, greatly reducing interruptions to daily data processing and access, supporting business continuity, and containing operational costs.

One of the greatest risks that IT can introduce to banking is inadequate use of capabilities offered by the constant improvement process taking place in this area, and consequently reduce the bank's competitive power. Therefore, from the risk management point of view, it is necessary to view IT operations as a whole, and information security management as a part of that whole. Bielski (2008) states that some think of business continuity as doing what is necessary to set up a "shadow" organization that will take you from incident response through various phases of recovery. Winniford et al. (2009) pointed out that, there still exists ongoing debate as to the exact scope and overlap of several concepts such as ITSM, ITIL, SLM, CobiT and BSM. Pollard and Cater-Steel (2010) identified three critical success factors for successful ITIL implementations: Creating an ITIL-friendly culture, process as a priority, and customer-focused metrics. McNaughton et al. (2010) proposed a holistic evaluation framework for evaluating the extent to which ITIL best practices are successful in supporting business processes. Marten et al. (2010) studied the correlation between IT governance maturity and IT governance performance, while Spremic (2012) analised the IT governance maturity in banking sector in Croatia. Martinez and Williams (2010), Harindranath (2008), Foo and Witkowska (2008), Stanovnik and Kos (2007) considered several aspects of ICT in transition/emerging countries.

Business Continuity Institute (http://www.thebci.org) published in August 2010 a document on "BCM Legislation, Regulations and Standards" for a certain number of countries. According to this report, among the EU countries, only UK has defined full legislations regarding BCM. Other countries have partial regulations or standards on BCM, while Italy has no even a standard Netherlands has only an exact translation of ASIS Standard SPC.1-2009 - Organizational Resilience.

Bonin (2004) studied banking sector in four south-eastern European countries with each of them showing a different path in terms of privatization: Slovenia, Croatia, Bulgaria and Romania. Kraft (2004) conducted a study of challenges and accomplishments in banking reforms in south-eastern Europe. The challenges that the countries faced are as follows: A poor legal framework, an undeveloped market security, as well as a non-bank financial institution. Depending on country, these questions have been treated by some regulations on risk management. In Albania, for example, regulation on liquidity risk defined what contingency plan needs to contain. In other countries as well, there exists a similar situation, with more and less specified regulations only on contingency plans. However, as majority of banks operating in the SEE countries are originally from EU, the Contingency Plans are governed by the rules of a parent bank.

Various BCM and crisis management standards have been introduced over the last few years. Majority of these standards are countrywide, but the regulations are mandated by the central banks which means, that they specifies rules for the BCM in financial services. Table 2 depicts regulations and authorities for controlling their implementation in selected countries.

TABLE 2 - REGULATIONS AND AUTHORITIES FOR BCM PROCEDURES

Country	Regulation	Authority	Summary
Australia	APS 232	Australian Prudential Regulatory Authority (APRA)	APRA regulation for BCM in financial services firm
Bahamas	PU 19-0406 Supervisory and Regulatory Guidelines for BCM	The Central Bank of Bahamas	Apply to all commercial banks operating in the Bahamas, based upon Basel II
Brazil	NBR 15999-1 and NBR ISO/IEC 24672	ABNT	Straight translation of the BS 25999 and ISO 24672 standards
Canada	IDA By-Law 17.19 BCP	OSC (Ontario Securities Commission)	Establishing and maintaining BCP for financial services firms
China	a) HKMA BCP supervisory policy TM-G-2 b) IT Security Guidelines	a) Hong Kong Monetary Authority (HKMA) b) IT Services Dept. – The Government of Hong Kong Special Admin region	a) supervisory policies, minimum standards authorised institutions are expected to attain b) general concepts relating to IT Security
Croatia	a) Act on Credit Institutions b) Rules on adequate governance of IT	Croatian National Bank (CNB)	Set up a minimum control measures for proper IT Governance in banks and financial institutions. External and internal IS auditing mandated, reports provided to CNB.
EU Countries	High Level Principles for BC Basel II	Basel Committee on Banking Supervision	Principles that should be used internationally by financial regulators, addresses operational risk
India	India BCP	Reserve Bank of India (RBI) Securities and Exchange Board of India (SEBI) Bombay Stock Exchange (BSE)	Enforced by audit, requires need for BCP documentation and testing for least annually
Indonesia	Regulation No 9/15/PBI/2007, Indonesia BCP	Bank Indonesia	Implementation of Risk Management in the use of IT by commercial banks. Requires internal IS auditing
Japan	Manual for the Development of BCP in financial institutions BC at Bank of Japan	FISC (The Centre for Financial Industry Information System) BOJ (Bank of Japan)	Audit matter, corporate – wide testing at least annually
Malaysia	BNM/RH/GLO13-3 Guidelines on Management of IT	Central Bank of Malaysia	Enforces minimum BCM requirements, auditing mandatory

Continued from previous page

Russia	242-P	Bank of Russia	Banking internal control
Singapore	MAS BCM Guidelines Singapore Exchange BCM rules	MAS (Monetary authority of Singapore) SGX (Singapore Exchange)	7 guiding principles on executive responsibilities for BCM (testing BCP, setting RTO, etc.)
Switzerland	SFBC 06/6 SBA Self-Regulation	SFBC (Swiss Federal Banking Commission) SBA (Swiss Bankers Association)	Supervision of internal control and IS auditing Guidelines for BCM
Thailand	Thailand BCP	Bank of Thailand/Securities and Exchange Commission	Best practices for BC and DR in telecommunication industry
UK	BC Practice Guide BS 25999-1:2006 BS 25999-2:2007 BS 25777:2008 IT Service Continuity	FSA (Finance Services Auth.) Bank of England British Standards Institution	Guidance on BCM req. FSA based its BCM inspection on 7 Basel Forum principles
USA	Sarbanes-Oxley act SEC act ANSI/ARMA 5-2003 NYSE rule 446 etc.	PCAOB (Public Company Accounting Oversight Board)đ SEC (Securities and Exchange Commission) ANSI (American National Standards Institute)	Setting requirements for establishing sound BCM procedures, auditing needed.

Source: Research results

IV. NATIONAL REGULATIONS FOR BCM ACTIVITIES: CASE OF THE REPUBLIC OF CROATIA

The most common reason for conducting information system auditing is based on regulatory requirements. In the Republic of Croatia the regulatory framework for information system auditing was prescribed by Croatian National Bank. The main objective of the obligatory regulations is to effectively manage the level of operational risks, namely IT associated risk in credit institutions (banks, insurance, etc.). The Act about credit institutions and the Decision about appropriate management of information system are the cornerstones of the information system auditing regulation that obliged every credit institution to perform internal and especially external assessment of IT risks and to prepare a report for the regulator as well as for company's Board. The regulatory itself is concerned to a framework and scope of testing IT controls in order to be able to assess the level of specific IT risks. Regulatory framework prescribed the 18 areas which define the scope of every information system audit in the credit institutions in Croatia. These areas are as follows:

1. Managing information system security
2. Managing the risks associated to information systems
3. Managing logical and physical access rights
4. Managing the information systems assets
5. Managing operating and system records
6. Managing back-up and archive

7. Managing the relationships to service providers and outsourcers
8. Managing the relationships to hardware vendors
9. Managing the information system development
10. Managing physical security
11. Managing passwords
12. Configurations management
13. Change management
14. Business Continuity planning
15. Disaster Recovery plan
16. Managing incidents and problems
17. Antivirus policy
18. Documentation and internal acts associated to information systems

According to the regulatory framework, the board of every credit institution in Croatia is responsible for mitigating risks associated to every single area and to effectively manage the level of the acceptable IT risk. Some detailed and precise regulatory responsibilities include:

- To nominate the member of the Board who is responsible for managing and controlling information system
- To define information system strategy (due to 01.07.2008)
- To define clear and precise responsibilities for managing information system (01.01.2009)
- To nominate the autonomous CISO function (Chief Information Security Officer) (01.01.2009)
- To nominate the IT governance Committee (01.07.2008)
- To define the information system risk management methodology and processes (01.07.2009)
- To assess information system risks and to reduce them to acceptable level (01.07.2009)
- To classify and protect information (01.10.2009)
- Internal audit is responsible to conduct information system audits (01.01.2009)
- Board is responsible to establish the process of business continuity planning and management (01.07.2010)
- Board is responsible to create the business impact analysis, to accept the business continuity plan, to accept the disaster recovery plan and to test their functionality and effectiveness (01.07.2010)
- Board is responsible for establishing appropriate incident management process (01.07.2009)
- Board is responsible for establishing the process of data recovery which will be stored on the alternative location (01.10.2010).

In Croatia, internal and external IS auditing are conducted according to this framework, while Croatian National Bank monitors the whole process and fosters credit institutions to implement IS auditors' recommendation and secure the quality of IS audits. The main objective of such a strong regulation is to strengthen the maturity of IT governance processes in credit institutions. Some results of such approach may be the fact that all credit institutions in Croatia have a CISO (Chief Information Security Officer) as an autonomous person nominated for managing IS security. All of them are conducting IS auditing procedures and every single commercial bank operating in Croatia has to have BCP and DRP integrated into risk management process and IT governance policies.

Very strict and rigorous IT governance regulations in Croatia enforce that IS management is on very mature level in almost all commercial banks operating in the country. Consequently,

BCM practices are on very high level, meaning that every single commercial bank operating in Croatia has a BC strategy, BC plan and DR plan. Majority of them identified key IT control metrics for BCM (RTO, RPO) according to the business impact analysis. Also, majority of commercial banks operating in Croatia has a DR site and modern data replication systems. This is particularly interesting having in mind their ownership structure. Largest banks operating in Croatia are owned by banks with head offices in nearby countries (Italy, Austria, France, Germany), while in the same time, very strict regulations are meant that IT governance and BCM practices in their Croatian subsidiaries are much stronger than in parent companies. We can conclude that IT governance and BCM practices in the Republic of Croatia are much better than in majority EU countries. Therefore, such a regulation may be the model not just for nearby countries, but for the broader region (CEE region). The possible results of executive management activities in managing IT risk are presented in Table 3. IT governance and information system audit activities give a set of clear guidelines on how to manage IT risk for selected business process.

TABLE 3 - THE OUTCOME OF IT GOVERNANCE AND RISK MANAGEMENT IMPLEMENTATION

Key business process	Sales order (e-orders)
IT risk	System disruption
IT risk level	High – critical, Loss of data, corporate risk
Potential loss (BIA) (per day)	500.000 €
IT Risk Response Strategy	Immediate action, risk level reduction
IT (governance) goal	Number of hours lost per user per month due to unplanned outages
IT Control	CobiT 4.1 (*DS4, DS5*) ITIL *BCM* ISO 27001 (*10, 11, 4*)
Key Metrics – IT Control Efficiency	Availability >= 99,96% RTO < 3h RPO < 3h First Fix Rate > 90% MTTR < 30 minutes MTBF < 20 minutes
Detailed IT Metrics	• Percent of available service level agreements (SLAs) met • Number of business-critical processes relying on IT that are not covered by IT continuity plan • Percent of tests that achieve recovery objectives • Frequency of service interruption of critical systems
Responsible Person (Owner)	XY

Source: Research results

V. NATIONAL REGULATIONS FOR BCM ACTIVITIES: THE CASE OF BOSNIA-HERZEGOVINA

In Bosnia-Herzegovina (BandH) there are two mutually compatible banking sectors that follow its constitutional system based on two entities. In both entities (FBandH and RS) there exists independent Banking Agency dealing with supervision of banks' activities. Central Bank of Bosnia-Herzegovina (CBBH) coordinates the activities of the two Banking Agencies. CBBH prescribed minimum standards with regard to IT with the "Decision on the minimum computer configurations and the reserve location for the gyro clearing", as well as the "Decision on reserve ways of conducting gross settlement in real time" (GSRT). These decisions were made on November 19, 2004 and came into force on January 1, 2005. In January 2012 new regulatory provisions came into the force, but there were no time to investigate its usage.

According to these decisions, all commercial banks are required to make their own procedures for payment transactions in exceptional circumstances, in order to maintain continuity of payment transactions of the whole banking sector. However, Central Bank of BandH considered the issues of business continuity only in the area of payment transactions, without specifying details on how to achieve it. All banks are required to provide backup performance of payments in extraordinary circumstances, preferably in their own isolated location, or contract with another commercial bank. When it comes to backup site for payment transactions, CBBH prescribed only minimal computer configuration required for payment transactions under difficult circumstances, without specifying details about the isolated location. The aim of these decisions was not only to enable the continuity of payment transactions of individual banks, but to prevent endangering the entire banking payments sector. Business continuity is viewed as an aspect of the bank's operational risk management and it is defined by the "decision on minimum standards for operational risk in banks" in 2008. The banks are asked to provide daily backups, have safe backup location, as well as a plan for emergency situation aiming at ensuring business continuity. Bank is required to test its business continuity plan at least once a year. The decision itself in the creation of a business continuity plan lists only four items that must be represented, without any detailed specification of minimum standards that should be adhered during processes of writing and implementing a business continuity plan.

Maintaining business continuity of banks' activities in BandH is defined in a very poor way. Banking Agency of Federation of Bosnia and Herzegovina, namely the "Department of Banking Supervision" is in the process of preparing "Decisions on IT supervision" which would further specify the details about maintaining business continuity. It is expected that this decision will be completed and delivered to the banks by the end of this year. Smaller banks in general keep backup copies of data in one of its branches and business continuity in emergency circumstances is not fully defined. Banks with headquarters from EU have already completely defined and implemented their business continuity plans. Since the legal regulations in this field in BandH are not fully implemented, the banks are mostly working on the implementation of BCP solutions on the basis of the experience of neighboring countries, mainly Croatia, and legal regulations from the parent banks' countries. This is particularly the case when talking about several aspects of facility management and technology management in terms of a separate location for emergency situations. All banks were required to have a business continuity plan by the end 2008. As details about maintaining business continuity are not specified, we can see different ways of maintaining business continuity in BandH banking sector, and it depends on bank size, amount of capital and the origin of the bank.

VI. FRAMEWORK FOR IMPLEMENTATION OF BCM AND IT GOVERNANCE STANDARDS

By imposing the IT standards and regulations, the governments ask the banks to implement several methods of risk management. However, implementing these standards only is not enough in regard to business continuance of the banks. Business continuity today relies on a set of continuous computing technologies that provide an efficient operating environment for "always-on business". Continuous computing technologies that have to be considered for an efficient and effective implementation according to the model presented in Figure 1 include the following major technologies (Figure 2):

- Servers or server configurations. Having in mind the dominance of the client-server architecture in modern computing, the role of server configurations has become crucial from the business continuity perspective. Server processors and server configurations are designed, configured and implemented in order to enhance availability ratios.
- Server operating systems. Server platforms are run by server operating systems. Server operating systems are expected to provide high ratios in terms of availability, reliability, and scalability for server configurations running business-critical applications.
- Serverware solutions. In addition to the core server operating system, server operating system vendors include (bundle) several modules in order to enhance the capabilities of their operating systems called serverware solutions.
- System administration knowledge and skills. IT skilled and experienced system administrator can resolve many problems that occur on operating system level which is very important in reducing the time of system recovery. The same applies for network administrators as well.
- Server-based fault-tolerance and disaster-tolerance technologies. If an IT platform uses fault-tolerant technology, system can continue to operate even in case of some component's failure.
- Server clustering is used in order to resolve the problems of heavy workload and improve scalability performances of server configurations.
- Data Storage and Backup solutions. Technologies used for data storage, data backup and data recovery play crucial role in data management in the form of a secondary layer, in addition to primary data storage (hard disk).
- Redundant units such as a RAID disks, network cards, modems, switches, routers, are used in order to reduce (minimize) downtime in a way that redundant components are purchased, stored and used to replace the broken ones.
- Networking and security technologies. In case of any kind of glitch on data communication platform, be it network card, modem, router, broken communication line, as a result, the system is unable to transfer data. Therefore, network downtime caused by any kind of glitch is also considered as crucial problem in modern computing.
- Advanced technologies include technologies such as snapshoot mirroring, data vaulting, virtual tape backup, online backup, etc.

Implementation of all these continuous computing technologies together with IT standards and regulations provides an integrated operating platform for "keeping business in business" of modern banking sector as well, as banks' business-critical applications are: i) Installed on enterprise servers, ii) run by server operating systems, iii) supported by serverware components, iv) backed-up by storage/backup solutions, v) administered by system administrators and so on. In most cases, most of these continuous computing technologies are implemented as a result of imposing the IT standards and regulations by either government or

international institutions. These standards and regulations provide a framework for implementing these technologies.

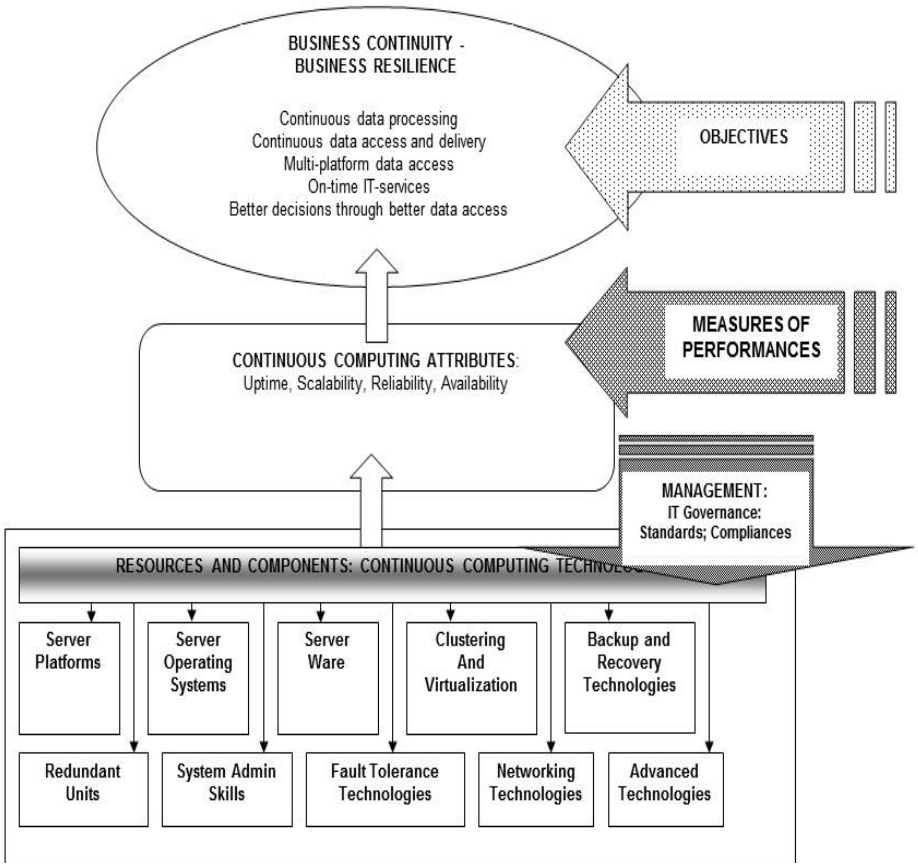

FIGURE 2. A SYSTEMIC MODEL OF BUSINESS CONTINUITY, CONTINUOUS COMPUTING TECHNOLOGIES AND IT REGULATIONS

Source: Authors' Model

VII. IMPLICATION FOR RESEARCHERS AND MANAGERS

In this paper we presented a systemic model of business continuity and continuous computing technologies which comprises the IT governance principles, namely IT regulation. Previous researches in this field were mainly associated to technological and managerial side of business continuity. We tried to fill the research gap by providing a research material which argues about the IT governance side of business continuity activities and its influence on growing business executives' interest on the matter. Therefore, after discussing theoretical background and analyzing literature review we construct, or rather comprehend our research model with the IT governance layer. As business continuity has been seen as one of main driver of operation risk, many businesses and industries was forced to develop efficient control countermeasures. Therefore, business continuity issues are no longer technological related problems and need

understanding and expertise of business executive level. IT governance methods and principles needs to be implemented namely in the form of developing solid and efficient control countermeasures in order to be able to manage risks associated to business continuity. By implementing IT governance principles, a company will develop a set of high level key risk indicators (such as RTO, RPO, availability rate, MTBF which are explained in further details in the paper). Such activities have to be initiated and managed by business executive's level and mainly driven by IT governance issues (regulations, compliance, risk management, business / IT alignment, etc.). Therefore, we hope that strong theoretical background provided in the paper, together with expert insight from real-word case studies would be of the researchers and managers interest.

VIII. CONCLUSIONS AND LESSONS LEARNED - FINDINGS FROM THE CASE STUDY

The findings obtained in the form of practical gains and recommendations can be summarized as follows:

- Both theoretical and conceptual considerations from the introductory sections and results from cases suggest a need to consider several IT-governance aspects when developing and implementing BC solutions in the banking sector and in general.
- The process of implementing BC and IT governance standards should be considered in a systematic way including both continuous computing technologies and IT standards and regulations.
- Information security is not only responsibility of the IT department, but it also includes many non-technological aspects: business continuity management, physical security and fraud risks. This proves that information security is a part of the integrated risk management process as a whole on company level whose structure has been explained in the risk management section. Therefore, the implementation of focused IT governance approach is of particular importance for managing IT risks.
- Two most frequently standard requirements for banking sector prescribed by the governments such as remote backup location and contingency plan should be only part of the integrated BC solution presented in this work.
- IT governance standards and regulations are considered in the form of a specific managerial action aimed at implementing continuous computing technologies for enhancing availability ratios of enterprise information systems.
- An enterprise information system must be managed from business continuity perspective in a way that it includes managerial and system administration activities related to managing the integration of business continuity drivers.
- The case study about Croatian IS auditing regulation framework shows that implementation of IT governance policies may reduce the level of IT risks and foster quality of IS environment. This is especially important when dealing with strategic IT risks such as BC and DR risks. In this light, the IT governance model for managing these risks is proposed and explained.
- As banking sectors in Croatia, BandH and other SEE countries are mostly based on the existence of EU-originated banks operating under Basel II, SOX and other standards, this sector is seen as one of the most developed in terms of BC/IT governance compliance in SEE countries. However, still a lot has to be done in the process of implementing integrated BC solutions. One possible model is explained in this work.

REFERENCES

Arduini, F. and Morabito, V. "*Business Continuity and the Banking Industry*", Communications of the ACM no. 53(3) (2010): 121-125.

Basel II. "*Basel Committee on Banking Supervision: International Convergence of Capital Measurement and Capital Standards: A Revised Framework*". June (2004): 177.

Bertrand, C. "B*usiness Continuity and Mission Critical Applications*". Network Security no. 20(8) (2005): 9-11.

Bielski, R. "*Extreme Risks, American Bankers Association*". ABA Banking Journal no. 100(3) (2010): 29-44.

Botha, J. and Von Solms, R. "*A Cyclic Approach to Business Continuity Planning*". Information Management & Computer Security no. 12(4) (2004): 328-337.

Cerullo, V. and Cerullo, R. "*Business Continuity Planning: A Comprehensive Approach*". Information Systems Management, Summer (2004): 70-78.

Churchman, C.W. "*The Systems Approach*". Delacorte Press, NY, (1968)

Craighead, C.W., Blackhurst, J., Rungtusanatham, M.J. and Handfield, R.B. "*The Severity of Supply Chain Disruptions: Design Characteristics and Mitigation Capabilities*", Decision Sciences no. 38(1) (2007): 131-155.

De Haes, S. and Grembergen, W.V. "*An Exploratory Study into IT Governance Implementations and its Impact on Business/IT Alignment*". Information Systems Management no. 26 (2009): 123–137.

Finch, P. "*Supply Chain Risk management*". Supply Chain management: An International Journal no. 9(2) (2004): 183-196.

Foo, J. and Witkowska, D. "*Transitional Progress and Business Challenge*" Int. Adv. Econ. Res (2008): 215-227.

Forrester Report. "*Businesses Take BC Planning More Seriously*", February (2009).

Gerber, M. and Solms, R. "*Management of risk in the information age*". Computers & Security no. 24 (2005): 16-30.

Gibb, F. and Buchanan, S. "*A framework for business continuity management*". International Journal of Information Management no. 26 (2006): 128–141.

Harindranath, G. "*ICT in a Transition Economy: The Case of Hungary*" Journal of Global Information Technology Management no. 11(4) (2008): 33-54.

IDC White Paper. "*Reducing Downtime and Business Loss: Addressing Business Risk with Effective Technology*". IDC, August (2009).

IDC Report. "*True High Availability: Business Advantage through Continuous User Productivity*", May (2006).

ITGI. "*Board Briefing on IT Governance*", 2nd edition. IT Governance Institute, Rolling Meadows, Illinois, SAD (2003).

Kadlec, C. "*Best Practices in IT Disaster Recovery Planning Among US Banks*". Journal of Internet Banking and Commerce no. 15(1) (2010): 1-11.

King, D.L. "*Moving Towards a Business Continuity Culture*". Network Security, Elsevier (2003): 12-17.

Kraft, E. "*Banking Reform in South East Europe: Accomplishment and Challenges*". OeNB Conference on European Economic Integration, Nov. 28-30, Vienna (2004).

Kuhn, J. R. Jr. and Sutton, S.G. "*Continuous Auditing in ERP System Environments: The Current State and Future Directions*". Journal of Information Systems no. 24(1) (2010): 91–112.

Marten, S., Pontus, J. and Mathias, E. "*The Effect of IT Governance Maturity on IT Governance Performance*". Information Systems Management no. 27(1) (2010): 10-24.

McNaughton, B., Ray, P. and Lewis, L. "*Designing an evaluation framework for IT service management*". Information & Management no. 47 (2010): 219–225.

Melton, A. and Trahan, J. "*Business Continuity Planning*". Risk Management no. 56(10) (2009): 46-48.

Pitt, M. and Goyal, S. "*Business Continuity Planning as A Facilities Management Tool*". Facilities no. 22(3-4) (2004): 87-99.

Pollard, C. and Cater-Steel, A. "*Justifications, Strategies, and Critical Success Factors in Successful ITIL Implementations in U.S. and Australian Companies: An Exploratory Study*". Information Systems Management no. 26 (2010): 164–175.

Spremić, M. "*Measuring IT Governance Performance: A Research Study on CobiT - Based Regulation Framework Usage*". International Journal of Mathematics and Computers in Simulation no 6(1) (2012): 17-25, ISSN: 1998-0159.

Spremić, M., Žmirak, Z. and Kraljević, K. "*Evolving IT Governance Model – Research Study on Croatian Large Companies*". WSEAS Transactions on Business and Economics no. 5(5) (2008): 244-253.

Spremić, M. "*IT Governance Mechanisms in Managing IT Business Value*". WSEAS Transactions on Information Science and Applications no. 6(6) (2009): 906-915.

Stanovnik, P. and Kos, M. "*Technology Foresighting in an Emerging Economy- The Case of Slovenia*". Economic and Business Review for Central and South - Eastern Europe no. 9(2) (2007): 165-182.

Turetken, O. "*Is Your Backup IT-Infrastructure in a Safe Location – A Multi-Criteria Approach to Location Analysis for Business Continuity Facilities*". Information Systems Frontiers no. 10 (2008): 375-383.

Van Grembergen, W. and De Haes, S. "*Measuring and Improving IT Governance through the Balanced Scorecard*" Information System Control Journal no. 2 (2005).

Winniford, M.A., Conger, S. and Erickson-Harris, L. "Confusion in the Ranks: IT Service Management Practice and Terminology". Information Systems Management no. 26 (2009): 153–163.

PRIMJENA IT STANDARDA UPRAVLJANJA I UPRAVLJANJE KONTINUITETOM POSLOVANJA U TRANZICIJSKIM EKONOMIJAMA: SLUČAJ BANKARSKOG SEKTORA U HRVATSKOJ I BOSNI I HERCEGOVINI

Sažetak: Tijekom proteklog desetljeća upravljanje kontinuitetom poslovanja se razmatralo uglavnom iz perspektive tehnologije ili planiranja. Ovaj rad ide korak naprijed i razmatra upravljanje kontinuitetom poslovanja sa stajališta IT upravljanja. Osim toga, ocjenjuju se i standardi te legislativa usmjerena poboljšanju stanja. Primjena najboljih sektorskih standarda i procesa kao što su ITIL i CobiT u kombinaciji s drugim IT rješenjima može dovesti do znatnog smanjenja rizika te smanjiti rizik poslovanja i time rezultirati smanjenjem nedostupnosti sustava. Istražuju se slučajevi primjene glavnih standarda informacijske tehnologije u bankarskom sektoru Hrvatske i Bosne i Hercegovine sagledani iz ove dvije perpektive.

Ključne riječi: upravljanje kontinuitetom poslovanja, IT upravljanje, IT rizici, IT revizija, nedostupnost, dostupnost


SVEUČILIŠTE JURJA DOBRILE U PULI
ODJEL ZA EKONOMIJU I TURIZAM
DR. MIJO MIRKOVIĆ
UTEMELJEN 1960.