International Journal of
Emerging Research in Management &Technology
ISSN: 2278-9359 (Volume-5, Issue-8)

Research Article

August 2016

Business Continuity Planning: A Study of Frameworks, Standards and Guidelines for Banks IT Services

Rupal Choudhary
Ph.D. Research Scholar, Dr. D.Y. Patil Vidyapeeth,
Pune, Maharashtra, India

Dr. (Col) Kunal Bhattacharya
Ph.D. Guide, Dr. D.Y. Patil Vidyapeeth,
Pune, Maharashtra, India

Abstract-

With the advent of IT services, the dependence of businesses on these services has increased significantly. It Services help the businesses in improving their efficiency and enhancing their organizational competitiveness. Because of the digitization of the businesses, IT has become an essential part for any organization. Financial Institutions (Banks) are one of the leading service industry relying heavily on the IT services for their day-to-day operations. Therefore, the importance of IT continuity, in case of any unforeseen situation, has become a point of critical importance. Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP), part of Business Continuity Management (BCM), are designed to ensure provisions for the critical business processes and IT systems within predefined recovery time frames. The designing and implementation of BCP for the banks' IT systems and services is not a one off exercise but an ongoing process. Various standards, frameworks and guidelines have been designed for the implementation of IT Business Continuity Plans in banks. Way back in 1998, the RBI had recognized the importance of BCP when it released a guidance note for bank management to evaluate the capability of controls in relation to risk related to Computer and Telecommunication systems. There are various practices of BCP to maintain the business continuity in the event of interruptions from man-made or natural disasters. This research paper focuses on global standards, frameworks and guidelines for designing and implementation of IT Business Continuity as a part of BCM in banks. Research paper is based on secondary data.

Keywords- Information Technology, Business Continuity Planning, Disaster Recovery Planning, Standards, Frameworks, Guidelines.

I. INTRODUCTION

Due to the e-business boom business continuity has been treated as both IT and managerial issues. Business continuity management as a separate IT-discipline emerged long years ago.

Business Continuity Management (BCM) is a management process that identifies risk, threats and vulnerabilities that could impact an entity's continued operations and provides a framework for building organizational resilience and the capability for an effective response.

The core documents of BCM are business continuity plan (BCP) and disaster recovery plan (DRP)

Disaster recovery which is often used interchangeably with BCP is defined as the rebuilding and recovery after a disaster (Cannon et al., 2006). Disaster recovery is one of the potential solutions to effective BCP (Eric et al., 2010).Disaster Recovery is a small subset of business continuity (Cannon et al., 2006).

BCM is the development of strategies, plans, and actions to protect or provide an alternative mode of operations for business processes that, if interrupted, could seriously damage or cause fatal losses to an organization. It includes BCP, DR and crisis management (Mark, 2008).

A business continuity plan (BCP) is to help ensure that business processes can continue during a time of emergency or disaster. Such emergencies or disasters might include a fire or any other case where business is not able to run under normal conditions.

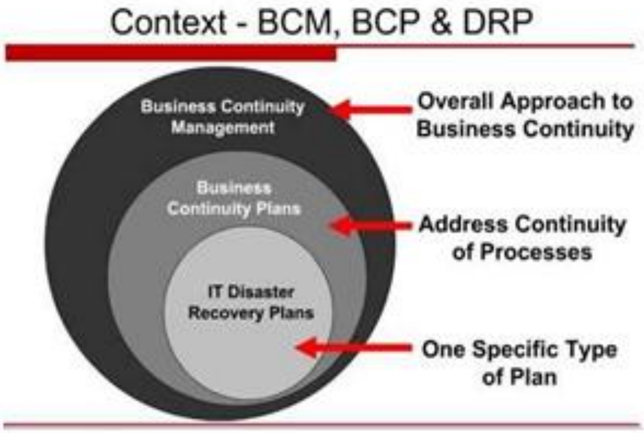

Context - BCM, BCP & DRP
Business Continuity Management
Business Continuity Plans
IT Disaster Recovery Plans
Overall Approach to Business Continuity
Address Continuity of Processes
One Specific Type of Plan

Figure 1: BCM, BCP & DRP Context

A disaster recovery plan (DRP) is a documented process or set of procedures to recover and protect a business IT infrastructure in the event of a disaster.

Over the past decade, the world has experienced a diverse range of disasters like tornados, tsunamis, droughts, cloud bursts, floods, cyclones, typhoons etc.highlighting the huge demand for Business Continuity.

II. RESEARCH METHODOLOGY

This research is based on secondary data. Secondary Data has been collected from previous research, online journals, and BCP consultant websites, annual reports of banks & institutes who are developing the standards, frameworks for the business continuity.

III. LITERATURE REVIEW

This literature review highlights the need and availability of standards, frameworks & guidelines for business continuity in the organizations.

Various events in recent years, particularly in connection with terrorism, pandemics and natural disasters, have highlighted the vulnerability of financial market participants and financial systems. Awareness of such events and their potential impact has increased significantly. [1]

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. [2]

To be most effective, BCP must be aligned with or complete against a standard, appropriate (fit for purpose), practical, realistic, up-to-date, effective and a plausible (proven) capability. [3]

As per the guidelines by Reserve Bank of India (RBI) the pivotal role that banking sector plays in the economic growth and stability, both at national and individual level, requires continuous and reliable services. Increased contribution of 24x7 electronic banking channels has increased the demand to formulate consolidated Business Continuity Planning (BCP) guidelines covering critical aspects of people, process and technology. [9]

The ISO 22301:2012, the world's first international standard for BCM has been established to assist organization minimizes the risk of business disruptions. The official title of this standard is "Societal Security - BCMS - Requirements". This new BCM standard was published on May 15, 2012 and will replace the current British Standard BS 25999 (St-Germain et al., 2012). The transition period endedin May 2014 when no new BS 25999 certification was issued. As for the existing BS 25999 certified organizations, the required transition was relatively straightforward and could be conducted at a future surveillance audit visit up until May 31, 2014.[12]

The presence of organization policy and framework will certainly support the implementationof DRP. Such as, learning and development policy, internal and external communications policy, management risk position, technical blueprint and technology process frameworks like System Development Life Cycle (SDLC) [13]

There are a number of policies and guidelines that exist for the organizations, to provide directions for information security. The commercial standard ISO-27000 series helps to build structures of a firm's security policy. Especially ISO-270002 (security controls), ISO-270031 (business continuity) and ISO-270032 (cyber security) are relevant to SMEs. [14]

Companies whose aim is to ensure the continuity of their business apply Business Continuity Management, usually through proven and certified standards and related norms. To eliminate threats from the external and internal environments, they use the valuable knowledge of their employees – specialists, without whom the companies would fail to ensure and implement these activities [15]

IV. FRAMEWORKS, STANDARDS AND GUIDELINES FOR BCP & DRP AS A PART OF BCM

A. IT Governance Framework

Develop a framework for IT continuity to support enterprise wide business continuity management using a consistent process. The objective of the framework should be to assist in determining the required resilience of the infrastructure and to drive the development of disaster recovery and IT contingency plans. The framework should address the organizational structure for continuity management, covering the roles, tasks and responsibilities of internal and external service providers, their management and their customers, and the planning processes that create the rules and structures to document, test and execute the disaster recovery and IT contingency plans. The plan should also address items such as the identification of critical resources, noting key dependencies, the monitoring and reporting of the availability of critical resources, alternative processing, and the principles of backup and recovery.

- Describe the conditions of plan before its activation
- Emergency Procedures and liasioning with appropriate authorities
- Identification of processing resources and locations
- Identification of information for backup and location for storage
- Resumption procedures and maintenance schedule
- Awareness and education activities
- Describing individual responsibility to execute a component of plan with alternatives

B. COBIT

Control Objectives for Information and Related Technology (COBIT) is a *framework* created by ISACA for information technology (IT) management and IT governance. It is a supporting toolset that allows managers to bridge the gap between control requirements, technical issues and business risks.

COBIT 5 provides a comprehensive framework that assists enterprises to achieve their goals and deliver value through effective governance and management of enterprise IT.

The governance system should consider all stakeholders when making benefit, resource and risk assessment decisions.COBIT 5 addresses the governance and management of information and related technology from an enterprise wide, end-to-end perspective as stated in principle 2 in Figure 2.

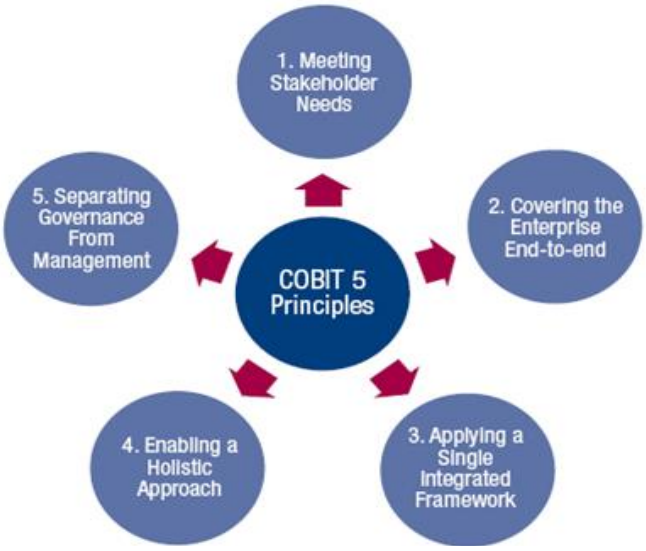

1. Meeting Stakeholder Needs
2. Covering the Enterprise End-to-end
3. Applying a Single Integrated Framework
4. Enabling a Holistic Approach
5. Separating Governance From Management
COBIT 5 Principles

Figure 2: COBIT Principles

COBIT 5 aligns with the latest relevant other standards and frameworks used by enterprises such as enterprise and IT related frameworks.

Factors that, individually and collectively, influence whether something will work—in the case of COBIT, governance and management over enterprise IT.

C. ITIL

ITIL, formerly an acronym for Information Technology Infrastructure Library, is a set of practices for IT Service Management (ITSM) that focuses on aligning IT services with the needs of business.

There are five stages in the ITIL Service Lifecycle:

1. Service Strategy
2. Service Design
3. Service Transition
4. Service Operation
5. Continual Service Improvement

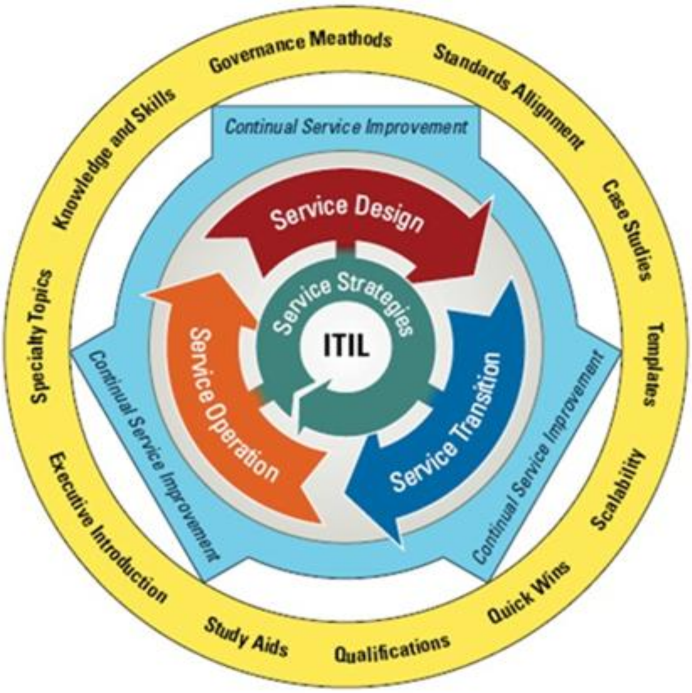


Figure 3: ITIL Framework

Benefits of ITIL

- Improve Resource Utilization
- Be More Competitive
- Decrease Rework
- Eliminate Redundant Work
- Improve upon project deliverables and time
- Improve availability, reliability and security of mission critical IT services
- Justify the cost of service quality
- Provide services that meet business, customer and user demands
- Integrate central processes
- Document and communicate roles and responsibilities in service provision
- Learn from previous experience
- Provide demonstrable performance indicators

COBIT and ITIL have been used by information technology professionals in the IT service management (ITSM) space for many years. Used together, COBIT and ITIL provide guidance for the governance and management of IT-related services by enterprises, whether those services are provided in-house or obtained from third parties such as service providers or business partners.

ITIL could be seen as the way to manage the IT services across their lifecycle, while COBIT is about how to govern the Enterprise IT in order to generate the maximum creation of value by the business, enabled by IT investments, while optimizing the risks and the resources. COBIT 5 describes the principles and enablers that support an enterprise in meeting stakeholder needs, specifically those related to the use of IT assets and resources across the whole enterprise. ITIL describes in more detail those parts of enterprise IT that are the service management enablers (process activities, organizational structures, etc.).[6]

D. BS25999 for DRP/BCP

The British Standards Institutions have also published a standard called BS25999 for DRP/BCP. The purpose of it is to “1) Provide a basis for understanding business continuity management, 2) Provide a means of measurement that is consistent and recognized, 3) Provide a system based on established good practice” (" What is BS25999", 2008)

E. ISO/IEC 27031:2011 Information technology — Security techniques — Guidelines for information and communications technology readiness for business continuity

ISO/IEC 27031 provides guidance on the concepts and principles behind the role of information and communications technology in ensuring business continuity.

The standard:

- Suggests a structure or framework (actually a set of methods and processes) for any organization – private, governmental, and non-governmental;
- Identifies and specifies all relevant aspects including performance criteria, design, and implementation details, for improving ICT readiness as part of the organization’s ISMS, helping to ensure business continuity;
- Enables an organization to measure its ICT continuity, security and hence readiness to survive a disaster in a consistent and recognized manner.

The standard encompasses all events and incidents (not just information security related) that could have an impact on ICT infrastructure and systems. It therefore extends the practices of information security incident handling and management, ICT readiness planning and services.

ICT Readiness for Business Continuity (IRBC) [a general term for the processes described in the standard] supports Business Continuity Management (BCM) “by ensuring that the ICT services are as resilient as appropriate and can be recovered to pre-determined levels within timescales required and agreed by the organization.”

ICT readiness is important for business continuity purposes because:

- ICT is prevalent and many organizations are highly dependent on ICT supporting critical business processes;
- ICT also supports incident, business continuity, disaster and emergency response, and related management processes;
- Business continuity planning is incomplete without adequately considering and protecting ICT availability and continuity.

F. NFPA (National Fire Protection Association)1600

The National Commission on Terrorist Attacks Upon the United States (the 9/11 Commission), recognized NFPA 1600 as our National Preparedness Standard. Widely used by public, not-for-profit, non-governmental, and private entities on a local, regional, national, international and global basis, NFPA 1600 has been adopted by the U.S. Department of Homeland Security as a voluntary consensus standard for emergency preparedness.

NFPA 1600 address provisions to cover the development, implementation, assessment and maintenance of programs for prevention, mitigation, preparedness, response, continuity and recovery.

G. ISO 22301:2012

ISO standards are a part of the key building blocks of BCM.ISO 22301:2012 specifies requirements to plan, establish, implement, operate, monitor, review, maintain and continually improve a documented management system to protect against, reduce the likelihood of occurrence, prepare for, respond to, and recover from disruptive incidents when they arise.

The requirements specified in ISO 22301:2012 are generic and intended to be applicable to all organizations, or parts thereof, regardless of type, size and nature of the organization. The extent of application of these requirements depends on the organization's operating environment and complexity.

Benefits of ISO 22301:2012

- Identify and manage current and future threats to your business
- Take a proactive approach to minimizing the impact of incidents
- Keep critical functions up and running during times of crises
- Minimize downtime during incidents and improve recovery time
- Demonstrate resilience to customers, suppliers and for tender requests

H. NIST (National Institute of Standards and Technology)

National Institute of Standards and Technology (NIST) is responsible for “developing standards and guidelines for providing adequate information security for all operations and assets”

NIST has a series of Special Publications (SP) and Federal Information Processing Standards (FIPS) that provide federal agencies with standards and guidelines for most aspects of information systems security.

NIST SP 800-34 – Contingency Planning Guide for Information Technology (IT) Systems -was first published in June 2002, and provides instructions, recommendations, and considerations for government IT contingency planning.

Contingency Planning refers to interim measures to recover IT services following an emergency or system disruption.

While designed for federal systems, NIST SP 800-34 has been used as the guideline for contingency planning throughout much of the private sector.

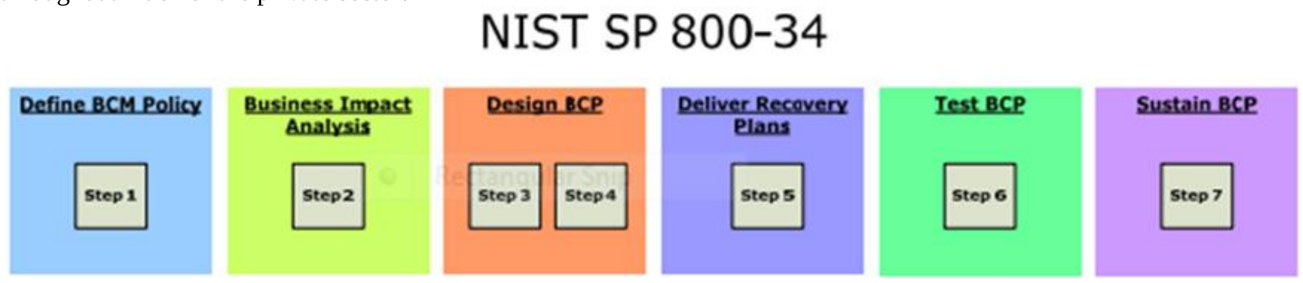


Figure 4: Process Map

I. Six steps BCP/DRP framework by Ian Storkey[4]

1. Document business activities and critical processes and systems
2. Undertake business impact analysis to assess probability and impact
3. Develop BCP/DRP (include 3rd parties)
4. Implement or update BCP/DRP
5. Training to imbed into the day-to-day operations of the ministry of finance
6. Regular (annual) testing and updating

Banks should consider various BCP methodologies and standards, like BS 25999, as inputs for their BCP framework.[7]

J. RBI Guidelines for Indian Banks [9]

Senior Management is responsible for prioritizing critical business functions, allocating knowledgeable personnel and sufficient financial resources to implement the BCP

- Senior official needs to be designated as the Head of BCP
- All departments to fulfill their respective roles in a co-ordinated manner
- Adequate teams for various aspects of the BCP at Central Office, Zonal/Controlling Office and branch level
- Banks should consider various BCP methodologies and standards
- BCP to include measures to identify & reduce probability of risk
- Vulnerabilities should be incorporated into the Business Impact Analysis
- People aspect should be an integral part of a BCP.
- Pandemic planning needs to be incorporated as part of BCP framework

The RBI in its Guidance note on “Management of Operational Risk” [2005] has stressed the need to establish a disaster recovery and BCP for technology related risks as a part of ORM framework. The RBI, in its circular on operational risk management and business continuity Planning” [2005], clearly states that the responsibility for effective migrated BCP rests with the Board of Directors and the management and has listed a set of minimum requirements for effective BCM by banks. The circular also required banks to disclose information relating to major failures of critical systems customer segment/services impacted due to failures and steps taken to avoid such failures in future. The RBI, in its guidelines on "Outsourcing of Financial Services by Banks" in 2005, has mandated banks to ensure that the service provider has a BCP and the same is regularly and maintained.

In many cases, an organization may elect to use an outsourced disaster recovery provider to provide a stand-by site and systems rather than using their own remote facilities. In addition to preparing for the need to recover systems, organizations must also implement precautionary measures with an objective of preventing a disaster in the first place. These may include some of the following:

- Local mirrors of systems or data. Use of disk protection technology such as RAID
- Surge protectors—to minimize the effect of power surges on delicate electronic equipment
- Uninterrupted power supply (UPS) or backup generator to keep systems going in the event of a power failure
- Fire preventions—alarms, fire extinguishers
- Anti-virus software and security measures

A disaster recovery plan is a part of the BCP. It dictates every facet of the recovery process, including:

- What events denote possible disasters;
- What people in the organization have the authority to declare a disaster and thereby put the plan into effect;
- The sequence of events necessary to prepare the backup site once a disaster has been declared;
- The roles and responsibilities of all key personnel with respect to carrying out the plan;
- An inventory of the necessary hardware and software required to restore production;
- A schedule listing the personnel that will be staffing the backup site, including a rotation schedule to support ongoing operations without burning out the disaster team members.

Technology Solution Architecture to address specific BCM requirements are:

- Performance
- Availability
- Security and Access Control
- Conformance to standards to ensure Interoperability

K. Basel II: Providing a base for Business Continuity Management [11]

Basel II is the guidelines provided to the banks in order to defend them from operational and financial risks that they can face. Basel committee also issued documentation i.e. "Sound Practices for Management & Supervision of Operational Risk" to incorporate sound practices in different areas related to Operational Risk.

One such area is Business Continuity. There are certain principles in this documentation which provide the guidelines perform analysis & potential impact of risks that can take place. Not all the principles but some strictly emphasize on such parameters:

Principle 1: Awareness of Board of Directors regarding operational risk

Principle 3: Senior management responsibility for operational risk management framework implementation, generating awareness and policy development "…Clear strategies and oversight by the board of directors and senior management… is all crucial elements of an effective operational risk management framework for banks of any size and scope ."

Principle 7: The focus is on contingency planning and business continuity planning: "…Banks should have in place contingency and business continuity plans to ensure their ability to operate on an ongoing basis and limit losses in the event of severe business disruption."

Principle 9: Management's role in evaluating operational risk management policies, procedures, and practices. The reason to include these principles here is that there is a relation between Operational Risk and Business Continuity. Basel committee defines operational risk as: The risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. Basel committee also specifies seven specific risk event categories. Among these seven categories, three directly relates to business continuity:

- Employment practices and workplace safety
- Damage to physical assets, caused by environmental and man-made events
- Business disruption and system failures (caused by hardware, software, network and utility issues).

Basel committee on e-banking requires that the banks must have effective capacity, business continuity and contingency planning processes to help ensure the availability of e-banking and services. It also underlines that the banks should ensure periodic audits about business continuity.

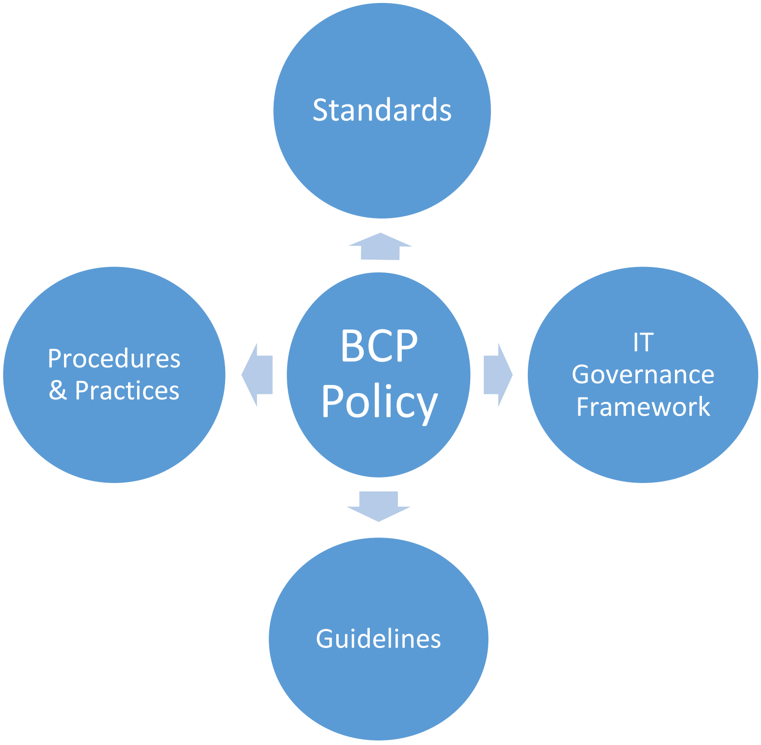
V. CONCLUSION

There is a need of BCP in banking sector for the continuation of the services during and after unforeseen interruptions.

Different frameworks, standards, and guidelines are available to implement Business Continuity Planning for IT services of the banks. Standards specify the use of specific technologies, tools in same manner. Standards help to ensure the quality practices. Standards help to maintain uniformity throughout the banks.Good Governance covers some level of compliance with established procedures, controls or standards. Framework is a series of documented processes which are used to define policies and procedures.

BCP provides benefits to the banks especially at corporate and branch levels to minimize disruptions and economic losses from disasters.

Selection of suitable frameworks, standards and guidelines are the responsibility of the top management at the time of planning and implementing the key components of BCP. Success of BCP & DRP policy is depend of factors like selection of suitable standard, framework, procedures, guidelines and practices shown in figure 5.



VI. FUTURE STUDY

Banking without IT services is not possible in today's IT world. Banks commitment of business continuity and disaster recovery of IT based services are highly depend on best suitable Information Security and business continuity policies, standards, frameworks, good practices and guidelines. IT governance frameworks are providing a logical structure to design and implement policies and standards for business continuity and disaster recovery in the banks.

In this paper researcher focused on available standards, policies and frameworks for business continuity and disaster recovery for the banking sector. Further study can highlight thechallenges   and issues of successful implementation of Business continuity and disaster recovery practicesfor banking organizations.

REFERENCES

[1] Swiss Banking, Recommendations for Business Continuity Management, August 2013

[2] Mario Spremić, Nijaz Bajgorić , Lejla Turulja , "Implementation Of IT Governance Standards And Business Continuity Management In Transition Economies: The Case Of Banking Sector In Croatia And Bosnia-Herzegovina", ECONOMIC RESEARCH ,ISSN 1331-677X print 2013 Volume 26 (1): 183-202

[3] Institute of Business Continuity Management, 2012

[4] Ian Storkey ,Operational Risk Management (ORM) and Business Continuity Plans (BCP), Economic Policy and Debt Department, The World bank

[5] Vlasta Svata , "System View of Business Continuity Management" , JOURNAL OF SYSTEMS INTEGRATION 2013/2

[6] NH Learning Solutions, 2015 http://nhlearningsolutions.com/Blog/TabId/145/ArtMID/16483/ArticleID/1514/COBIT-vs-ITIL.aspx

[7] RBI Guidelines, Electronic Banking Working Group, Gopalkrishna Committee, 2011

[8] Comparison of ITGovernance framework-COBIT, ITIL, BS7799, http://www.slideshare.net/meghnaverma3956/comparison-of-it-governance-frameworkcobit-itil-ds

[9] RBI Guidelines, https://www.rbi.org.in/scripts/PublicationReportDetails.aspx

[10] Nagoya Institute of Technology, Diversifying Options for Business Continuity Planning (BCP) / Business Continuity Management (BCM) and Emerging Needs for Economic Incentives - Tools Available in the Market and Japanese Scheme for Financial Incentives, APEC 2011.

[11] Preetish Ranjan, Prabhat Kumar & Kumar Abhishek , “Business Continuity Planning in Indian Perspective” Journal of Advances in Computational Research: An International Journal Vol. 1 No. 1-2 (January-December, 2012)

[12] Zahari Abu Bakar, Noorulsadiqin Azbiya Yaacob, Zulkifli Mohamed Udin, “The Effect of Business Continuity Management Factors on Organizational Performance: A Conceptual Framework,” International Journal of Economics and Financial Issues, 2015, 5(Special Issue) 128-134.

[13] Leong Lai Hoong & Govindan Marthandan, “Critical Dimensions of Disaster Recovery Planning, International Journal of Business and Management”; Vol. 9, No. 12; 2014 ISSN 1833-3850 E-ISSN 1833-8119

[14] Nabila Amrin, University of Twente, “The Impact of Cyber Security on SMEs”, 2014.

[15] H. Urbancova, and J. Urbanec ,“Knowledge Continuity as a Part of Business Continuity Management”, World Academy of Science, Engineering and Technology Vol:7 2013-04-24

[16] COBIT Framework, http://www.isaca.org/