Repercussion of program generated objects in smooth operations running from disaster recovery site

Muhammad Junaid Ashraf and Mohammad Altaf Mukati
SZABIST, Karachi Pakistan
m_j_ashraf@hotmail.com and altaf.mukati@szabist.edu.pk

***Abstract*— The disaster could happen at any point of time and due to which there could be financial loss in addition to operational loss, considering 24/7 banking environment and having its branches in different parts of world. The risk involved in financial loss may be very high and could result in unbearable loss. In such cases where organizations have zero downtime and having high availability of data, the disaster recovery mechanism and data replication scope has to be well defined and should be strictly followed. Assuming that the network, storage and hardware is available at DR site and the replication of critical data is also verified but still there are several objects left behind which were not covered under replication scope. These objects were created by programs themselves while executing (not in replication scope). In such case the successful switch might not be called as successful because those objects will not be available at DR site and may lead to business interruption or financial loss. This problem arises when developers have access on production servers and they create new libraries/objects for their program execution without informing the implementers through proper change management process. In this paper we will provide the guidelines and framework for deployment of programs on production servers also the guide for smooth switching (change of role) of entire core banking environment running on IBM System-i to DR site.**

Keywords— IBM System i; AS/400; MISYS; MIMIX; Disaster recover; Change management; Objects and libraries.

I. INTRODUCTION

Continued business operations and high availability of IT infrastructure including business applications, communication network and hardware are the major concerns in case of any disaster [1-2]. The risk factors in banking sector is very high due to fact that in case of disaster there could be financial loss and to minimize such losses disaster recovery mechanism parameters should be well defined [3-11].

There are two broader design goals that need to be focused while designing the Disaster Recovery System i.e. Recovery Time Objective (RTO) and Recovery Point Objective (RPO) [3] accordance with Business Continuity Process Management. Disaster recovery requirement is based on RTO and RPO and these values should be considered prior as the business may be affected and there are chances of financial loss. Both RTO and RPO are services of Business Continuity Process Management (BCPM) [6]. RTO is time recovering from disaster in case of whole site failure; while RPO is the loss business can tolerate.

IBM Power 7 machines has the capability to provide high available system, Power 7 machines are virtualized machines and the resources of the systems are separated, so no intervention can be possible that would result in business interruption.

II. IBM SYSTEM I BRIEF INTRODUCTION

After System/36 IBM introduced AS/400 in 1988 which runs on Operating System/400 or OS/400. OS/400 is object based multi-user OS with the IBM DB/400 & Query/400 built into it. IBM System i supports many program languages include RPG, COBOL, Perl, Java, C, C++ and Pascal. These program languages require their compiler. The Integrated Language Environment (ILE) support C, C++, CL, RPG, FORTON and COBOL [1].

Power Systems allows multiple virtual systems to run on a single hardware footprint, eliminating the need the additional hardware. The next generation is come up with the capability to support fully virtualized hardware. The new Power 7 machines can support both System i and System P. LPAR can be created to separate the resources of each machine. The virtualization of Power machines supports network virtualization, memory virtualization and processor virtualization [1,12-16].

Journals, for other platforms known as Logs, are used to track the changes in the objects. The remote journaling is used for implementing those changes to remote server or DR server [17]. Subsystem is to dividing the system into subsystem where system resources are assigned to optimize workload by distributing the resources as per application or job needs. Properties and components of subsystems are defined in the subsystem narrative [7]; these include the subsystem name, for example: QCTL for the managing and controlling subsystem, QINTER for the interactive subsystem and QBATCH for the batch subsystem

A. Type of Jobs

There are generally two types of jobs Interactive and Batch as shown in Table 1.

B. System Values

These values are control and configuration attributes which allow to control and/or customize certain OS functions. Following are the types described briefly [16]:

- *ALC (Allocation Values):-Control No. of active jobs how much main storage will be used to run jobs.
- *DATTIM (Date and Time):-to configure the date and time of the system.
- *LIBL (Library List):- Define the system library list i.e. group of libraries a uses to search for objects it needs for processing.
- *EDT (Editing values):- Controls how dates, decimal values and numbers involving currency symbols are formatted.
- *MSG (Messaging and Log Values):- how system handles and records certain type of messages.

- *SEC (Security Values):- Concerned with security for e.g. Maximum numbers of invalid sign on attempts allowed.
- *STG (Storage System Values):- Defines minimum size and number of active jobs of the base storage pool.
- *SYSCTL (System Control Values):- Define or obtain controlling values of the OS, user assistance level, operator console name and date & time to automatically IPL (Initial Program Load) the system.

Note: Initial Program Load (IPL) is a boot process which loads the OS when the power is turned on.

Table 1: Types of job

INTERACTIVE	BATCH
All interactive jobs begins when users' sign on and terminates when signs off, it's like a conversational mode between system and user both interact with each other, there is always a sort of interchange between user and program, utility or OS functions. Because of its interactive nature, sometimes it locks the workstation keyboard until the requested is completed, for alternate we have batch job.	Runs in the background, without user intervention. Doesn't require controlling or any input values to be entered through workstation once started. Has a job queue, managed by subsystem, batch job waits in line for its turn, although priority can be set accordingly which job you want to be finish first.

C. Disaster Recovery

Disaster recovery is a science which helped organizations to recover from a disaster with or without any tolerable loss. The disaster recovery solutions mostly consist of software which keeps tracking and monitoring the primary site and secondary site [3]. Following points were generalized for unsuccessful disaster recovery:

- Lack of a plan to recover successfully from potential disasters and other unplanned interruptions
- Need to identify gaps in disaster planning
- Lack of established recovery plans for multivendor data systems
- Need to comply with regulations

III. CURRENTLY DEPLOYED DR MECHANISM

Several kinds of disasters may happen at any point in time there would be environmental disaster, OS/Software crash, power failure, viruses' attacks unavailability of communication network and act of God, these disasters may lead the organization to not only business interruption but also impact the business integrity in term of customer satisfaction. The risk for data integrity is very high and cannot be tolerate if the organization is financial institute like banking sector. In banking sector, the data integrity is the major issue in case of disaster.

Disaster recovery is a science which helped organizations to recover from a disaster with or without any tolerable loss. The disaster recovery solutions mostly consist of software which keeps tracking and monitoring the primary site and secondary site [3].

Following points were generalized for unsuccessful disaster recovery:

- Lack of a plan to recover successfully from potential disasters and other unplanned interruptions
- Need to identify gaps in disaster planning
- Lack of established recovery plans for multivendor data systems
- Need to comply with regulations

Currently the DR solution is provided by IBM and replication software is used for DR is MIMIX. MIMIX has the capacity to switch the environment to DR automatically and it be set to manually. Currently the BANK is set the configuration to switch the environment manually because if network glitch occurs, MIMIX assumes it's a disaster and automatically switches the environment to DR site. To avoid this situation the configuration are set to manual. The higher management has the authority to announce the disaster. Once the disaster was announced then the environment was shift to DR site. Before that little information was collected. That information includes the current status of MIMIX data group either they synced or not. If the Data Groups are synced then environment successfully switched to DR. this is happen only in case of planned activity. Imagine if there is an unexpected failure and unplanned switching is required. In that case, the MIMIX data group must always be synced.

IV. USER ACCESS LEVELS

The user profile roles and responsibilities which are involved in the various processes in Bank's AS/400-iSeries Environment are defined as follows.

- System Administrator - *SECOFR Class – Remains Disabled
- System Administrator - *PGMR Class
- Security Officer
- Shift System Administrator
- System Operator
- Print Shop Operator
- System Programmer
- Branch User

V. IDENTIFYING THE DEPLOYING PROGRAM WHICH ARE CREATING LIBRARIES

There are various ways to identify the programs that are using CRTLIB function, QA team has to go to Program Development Manager (PDM) section of system to check the details of programs.

The QA team required to have the following information once they received the CMF:

- Source file name
- Library in which the source file existed

- Program name which needs to be deployed on production
- Source machine name

STRPDM command will be used to enter in PDM menu as shown in Fig. 1.

Table 2: Secofr user properties

S.No.	Special Authority	Description
1	*ALLOBJ	*ALLOBJ authority means that user can access any resource presented in the system, these resources are also known as objects.
2	*SECADM	Can change user profile settings, profile deletion and configuration.
3	*JOBCTL	Provide access to jobs running in the system.
4	*SPLCTL	Provide user to access and control output queues and job queues in the system.
5	*SAVSYS	Provide privileges to user to save, restore, and free storage for all objects on the system, whether user have access on particular object or not.
6	*SERVICE	Provide user to access and display the service function.
7	*AUDIT	Provide user the ability to change auditing features of the system.
8	*IOSYSCFG	System I/O configuration access.

Table 3: System programmer responsibilities

New Application Development	Any new addition to the core banking application or a new application component to support the core banking system.
Maintenance of Existing Application	The maintenance of the existing application components on the request of the business team.

If QA team found the function of CRTLIB is used in program and pointed to use libraries other than defined, then ask to CMF owner to remove this statement from the program code and if required then requested library should be the part of CMF and must be created by Administration team because System Admin team are responsible and authorized to create any library.

VI. DEVELOPERS' ACCESS ON PRODUCTION MACHINES

The access level of users on production environment must be compliance by the regulated guideline and would be good if the customer follows the IBM provided best practices for user security level, as discussed earlier in User Access Level section.

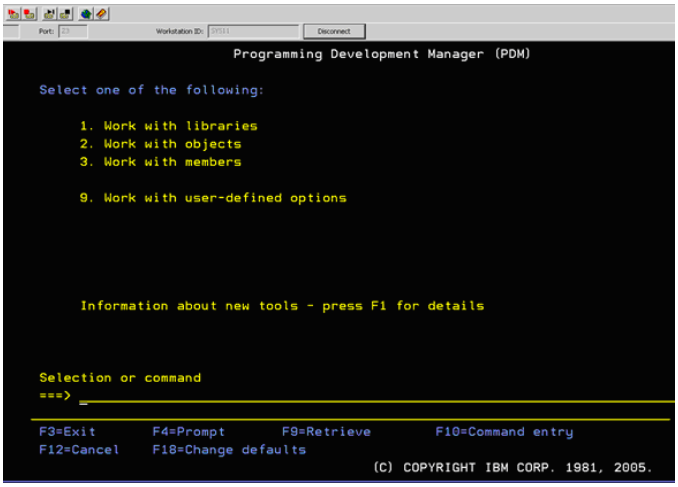

Fig. 1. Program development manager menu

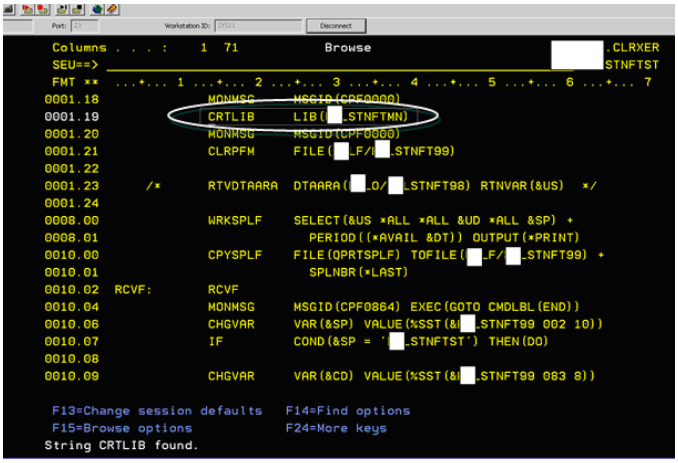

Fig. 2. Program code browser showing CRTLIB function found in code

Unauthorized access of IT systems will always led to failure and will definitely causes the operating loss as well financial loss. Having access on production machines is like creating the vulnerability by ignoring the security and data integrity concerns. It is highly recommended that developers must not have access on any of production servers and if access is required on account of business need and or any upgrade in the core application, proper approval process must be followed, the change management process must also be accompanied.

The purpose of disaster recovery site is to have a standby secondary site which will help the organization to recover from disaster. Establishing a DR site requires a huge investment, imagine the case of banking sector where banks need their financial data intact and highly available in case of nay failure. The problem arises when developers made changes in the system and do not inform the implementers or administrators. Also they made the required changes without following the proper change management process.

To overcome this situation following suggestions should be consider:

- There must be Quality Assurance (QA) team exist.
- Any change must be passed to QA for testing and evaluation
- The QA team has to analyze the deploying program and its impact on business application

- Must assure if the program creating the library, the desire library has to be added in MIMIX replication scope
- MIMIX replication scope has to update after the execution of change request

By doing so, any change will be reflected in DR site and there should be no disruption in business operations.

VII. MIMIX REPLICATION SCOPE

Replication scope is a data group which has a list of libraries and objects that should be available on DR site and must be replicated. The critical libraries and objects are added in MIMIX replication scope by the system administrator. Replicating the complete system is not a good solution rather selecting the critical application and data for replication.

MISYS have two major categories of libraries, Application libraries and Financial libraries. All the application related objects are saved under following libraries [14]:

- KAPBASEE
- KAPBASEFIL
- KAPBASEINP
- KAPEBASELIB
- KAPBASEWRK

While all the financial transactions are stored under following libraries:

- KFILXXX
- KLIBXXX
- KWRXXX
- KINPXXX

The in-house build application can use libraries other than MISYS provided, but their financial libraries must be the default libraries. There are scenario exists where organization used their own libraries for in-house build application. Like cheque book issuer program, tax deduction program, ATM fee charges program, etc.

Following suggestions would help to overcome the issues related to MIMIX replication:

- QA and business team has to align and identify which program has less impact on business
- Less impact application can be replicated once a week rather daily basis
- QA team has to identify which library needs to be replicate on DR site
- There should be separate Data Group for each unit
- Libraries should be fixed
- Libraries should be department specific

VIII. PROPOSED CHANGE MANAGEMENT PROCESS

Every organization required some changes either to enhance business or to upgrade their business application or hardware. These changes can be from business need and sometime changes are required because of any up-gradation of the system, patch implementation and any other major or minor demand of the configuration.

For larger organizations like BANK, the changes are at an increasing pace, which requires hundreds of changes to be managed, often with complex and changing deployment processes. For frequent changes and if the no. of changes are high then there would be need of standard change management process [13]. As time passes the IT infrastructure is also required maintenance, upgrades or fine-tuning.

The objective of standardized change management process is to:

- Ensure formally documented change management process existence and maintained
- Ensure that all changes are properly raised and approved prior to implementation
- Ensures that all the changes are scrutinized by Quality Assurance team prior to implement
- Ensure that all changes made to application or systems are tested on development environment before being placed to production
- Ensure that all changes can be easily back tracked
- Ensure that all changes are informed to respective stakeholders
- Ensure that all emergency changes are logged, managed and tracked

Following is the change management process that is being followed currently.

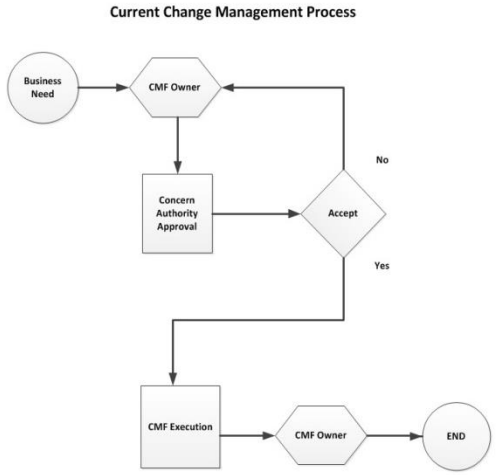

Fig. 3. Current change management process

In current practice there is no QA evaluation. Based on the issues with the currently deployed change management process which do not have any risk management. All the changes are directly deployed to production without the QA analysis. Following is the proposed change management process.

In proposed process, the Change will be evaluate and recommendations will be carry forwarded to concern authorities for the approval. Once the approval is granted then the changes will be performed on production environment.

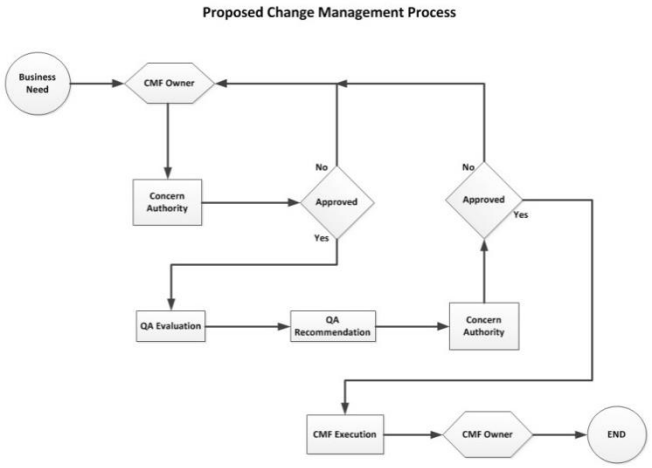

Fig. 4. Proposed change management process

CONCLUSION AND FUTURE WORK

The change management process and quality assurance parameters must be incorporated. Currently the BANK is having paper based environment and all the change requests are initiated and managed on papers, the issue with the paper based is not only high cost but also back tracking is very difficult. The BANK should apply the ITIL framework and must use paperless solution for automatizing the change process.

The BANK is using in-house developed application for libraries and objects' matching with production and backup servers. The report is generated on weekly basis because of its lengthy running time (5 hours approx.). Significant reduction in running time is not possible because the objects were locked while in use hence objects cannot be compared during office hours and EOD process. The only solution is to have QA introduced and enforces the developers not to use CRTLIB function in programs rather if required the libraries must be created by system administration team.

ACKNOWLEDGMENT

I would like to thank Dr. Mohammad Altaf Mukati for sparing his valuable time to give me proper guidelines on Independent Study. His kind support, co-operation and proper guidance have let me fully understand the work and I was able to complete my IS with full confidence and dignity. Also I would like to thanks to my colleagues for supporting me to complete this report.

REFERENCES

[1] IBM System i, http://www-03.ibm.com/systems/i/
[2] Honglin Han, Lin Li and Dehai Zhu, "Research and implementation on Remote Disaster Recovery System", International Conference on Computer Science and Service System, 2012
[3] B. Chad, "The Disaster Recovery Plan", SANS Institute, 2003.
[4] David Sandifer, Ken Brown, Joe Burns, Susan Crowell and Tim Kramer, "IBM Eserver iSeries Systems Management Handbook", Red Paper, 2005
[5] Brandon Schulz, Giancarlo Omati, Morten Buur Rasmussen Johnnie Talamantes, Claudio Villalobos and Brian Younger, "IBM Systems Director Navigator for I" RedBooks, 2009
[6] Th. Lumpp, J. Schneider, J. Holtz, M. Mueller, N. Lenz, A. Biazetti and D. Petersen,"From high availability and disaster recovery to business continuity solutions", IBM SYSTEMS JOURNAL, VOL 47, NO 4, 2008
[7] Frank G. Soltis, "Inside the AS/400" Duke Communications, 1995.
[8] http://www-01.ibm.com/software/success/cssdb.nsf/CS/STRD7JHM8E?OpenDocument&Site=default&cty=en_us, (Accessed on 19 Feb 2014)
[9] Charlotte Brooks, Matthew Bedernjak, Igor Juran and John Merryman, "Disaster Recovery Strategies with Tivoli Storage Management", IBM Redbooks, 2002
[10] T. Adeshiyan, C. R. Attanasio, E. M. Farr, R. E. Harper, "Using virtualization for high availability and disaster recovery" IBM Journel of Research and Development, 2009.
[11] D. Clitherow, M. Brookbanks, N. Clayton, G. Spear, "Combining high availability and disaster recovery solutions for critical IT environments", IBM System Journel, 2009.
[12] http://www.misys.com/
[13] Claudio Bartolini and David Trastour, "A Solution to Support Risk Analysis on IT Change Management", IFIP/IEEE International Symposium on Integrated Network Management, 2009.
[14] MIMIX and Double Take, http://www.visionsolutions.com/
[15] Sambit Sahu, Prashant Pradhan, Anees Shaikh, On Improving Change Management Process for Enterprise IT Services, 2008.
[16] IBM Redbook, "IBM i 7.1 Technical Overview with Technology Refresh Updates, 2013
[17] IBM i Security Planning and setting up system security 7.1