DISASTER RECOVERY AND BUSINESS CONTINUITY (DRBC)

SkillWeed

OLAYINKA AKINFENWA

TABLE OF CONTENTS

INTRODUCTION

DRBC is also known as **CONTINUITY OF BUSINESS (COB)**

Every organization must ensure they have a well established /fully implemented DRBC plan. This is critical and can be the difference between the continued existence and demise of a business after a disaster.

IMPORTANT DEFINITIONS

Disaster recovery (DR): is concerned with how a business recovers immediately following a disaster. This refers to efforts directed at business recovery after a disaster.

Business continuity (BC): concerned with how a business minimizes the impact of a disaster. This refers to continuation/sustenance of business before placing the company to its normal business structure.

DRBC seeks to ensure that information systems are available and running at all times to support and enable business functionality and growth. Despite all precautions and preventive controls disasters can still occur. In such instances, the business continuity plan (BCP) should enable recovery of information systems within an acceptable time frame to avoid any serious damage to the business.

BUSINESS IMPACT ANALYSIS (BIA)

A BIA is the initial step in the development of a business continuity plan. This process involves the identification of those information technology applications or systems critical to the survival/continued operations of the business. It is the responsibility of the business (not IT) to define these critical applications. The participation of end-user departments is important. BIA development is the most important process in DRBC.

EXAMPLE OF A BIA

IT APPLICATION	RTO
SAP	24 hrs
UNIX	48 hrs
ORACLE	4 hrs

RTO = RETURN TO OPERATIONS. This refers to the maximum number of hours or days within which the system should be up and running (available to the business) after a disaster. From the above table, oracle application should be up and running within 4 hours after a disaster/interruption.

TYPES OF DISASTERS

1. Fire

2.Tornado

3.Flood

4. Hurricane

5. Terrorism

6. Earthquake

DRBC plan addresses these type of disasters.

MAJOR STEPS IN DRBC PLAN

STEP1: THERE MUST BE A DRBC PLAN

STEP2: THE CORE/MAJOR TO THIS PLAN IS A BIA.

The company must conduct a BIA analysis .The BIA drives which of the systems and applications are critical to the success of the organization. It is important to note that not all the systems/applications in an organization have the same level of criticality/impact in the event of a disaster.

Examples

ABC&Co

Application	Use	Owner	Revenue Impact	Regulatory Impact	Safety	Total	RTO
Oracle database	Houses customer addresses info.	Sales dept	3	1	1	5	48
SAP	Accounting system	Acc. dept	3	3	1	7	24
UNIX	Customer accounts	Distr. dept	2	1	1	4	4
Peoplesoft	Employee info.	HR	1	3	3	7	24

Criteria definition:
Low = 1
Medium = 2
High = 3

Revenue

Low = 100,000- 500,000

Medium = 600,000- 1000,000

High = 〉1000,000

RTO= for how long can this application be down before impacting business.

IMPORTANT

The responsibility to perform a **BIA** lies with the business and not IT.

The business understands better the impact/outage a system or application will have on their business. As such they should determine the expected RTO so as to minimize the impact of the disaster on the business of the organization. They also have a better understanding of the revenue impact of an outage.

In the course of performing a DRBC audit the IT auditor must request for EVIDENCE of the performance of a BIA .The risk of not performing a **BIA** is the recovery of an application that has little or no impact first.

STEP3: RANKING & SELECTION OF CRITICAL APPLICATIONS

From the BIA the organization must rank and select systems and applications that are critical to the survival of the business based on the RTO and revenue impact.

STEP 4: CALL TREE

The DRBC plan must also include names, pager numbers, and telephone numbers of members of the recovery team.

As an IT auditor:

a) ensure BIA was done

b) Recovery team members- look at whether members are still available-call numbers.

Note: it is important that public relations department responds to the media in time of disaster.

STEP 5: ESTABLISHMENT OF A DISASTER RECOVERY TEAM.

The key teams needed to help in the recovery process must be established .IT auditor in the course of an audit should ensure that each of the established teams in a DRBC are functional –Request for minutes of last meeting. Sample some members of the team requesting to know if they have clear understanding of their team's responsibilities.

Typical questions: Are you aware you're a member of this team. Do you have a clear understanding of your team objective. When did you last meet?

STEP 6: TEST SCRIPT AND TEST PLAN

The script needed to perform the recovery of some of the critical applications must be pre-defined and updated as changes occur.

Example 1

UNIX operation system- to perform the recovery of UNIX operating system specific scripts to perform this recovery must be documented on the DRBC plan. Run script to recover UNIX.

STEP 7: TESTING SCHEDULE

A schedule must be established for periodic testing to ensure that the organization will be able to perform a successful recovery during a disaster (MOCK TESTING).

STEP 8: THE RECOVERY LOCATION

a) Hot site- A hot site is a site that mirrors the exact software, hardware etc of a primary site, i.e in the event of a disaster a location that is established far away must have the same technology for immediate recovery.

In a hot site all you need is to take your tape and load it and you are ready to go. The IT auditor must ensure that the hot site is of a reasonable distance from the organization and the hot site must not be visible/never having a signpost, no telephone number, no address. The address of the hot site must however be clearly stated on the DRBC plan.

In almost 100 % of the cases the hot site is an external organization rendering the service to so many organization e.g. IBM, SUNGUARD.

b) Warm site- It is a location with network outlets but no software or hardware that mirrors perfectly the primary site. Wiring connections such as fax, telephone do exist in a warm site. It's possible to have both hot site and warm site .This may be located in another office of the organization away from the primary site.

c) Cold site- This is a work area with no technological facilities.

d) Reciprocal Agreement- occurs when two companies agree to use each other's facilities in the event of a disaster. The major deficient with this is the fact that it is not mandatory and is subject to availability of space.

STEP 9: REDUNDANCY

The following alternative must be clearly specified in the DRBC.

a) Alternative power supply grid: the objective of this alternative line is to ensure that when the primary line fails there is an immediate alternative line available for use.

b) Alternative telecommunication line; The above also applies to the telecommunication line e.g contract with another telecommunication carrier e.g. primary line is from Verizon and the secondary line is from Sbc.If the primary line fails the secondary line comes in.

STEP 10 : UPS: UNINTERRUPTED POWER SUPPLY

To ensure a safe shutdown of critical systems and applications a Ups must be installed.

STEP 11: GENERATORS

The organization must ensure provision of generator and generator must be tested for capability and readiness. E.g the generator can be tested every Thursday from 4-8 pm.

STEP 12: INSURANCE

The primary objective of insurance is to transfer risk involved in an unplanned event.As part of a disaster plan an insurance policy may be obtained to cover some of the losses.

STEP 13: THE DISASTER RECOVERY PLAN MUST EQUALLY STATE LIST OF MAJOR SUPPLIERS AND VENDORS SUCH AS:

1) software vendors
2) Hardware vendors
3) Emergency water supply (contractor)
4) Contract agencies(manpower etc)

STEP 14: A COPY OF THE DISASTER RECOVERY PLAN MUST BE KEPT OFFSITE.

SUMMARY

The role of an IT auditor in a DRBC audit.

1. Is there a duly signed, current, updated and approved DRBC plan: If not approved it means there is no plan.

2. Ensure a BIA was conducted

3. Ensure there is a list of critical applications with appropriate RTO

4. Ensure there is a CALL TREE: The auditor must select a sample of names and telephone numbers and ensure they are valid.

5. The auditor must select a sample from the CALL TREE to review the following:

   a) Are members' ware of their membership of an assigned DRBC TEAM?

   b) Do they have clear understanding of their roles and responsibilities?

   c) REQUEST to know when last the team met, request for minutes of last meeting.

6. The IT auditor must also validate the establishment of a test script for the listed critical application.

7. The IT auditor must also validate the existence of a test schedule

8. The IT auditor must obtain and review the various contracts e.g. Hot site contract, warm site contract, water supply contract, Alternative power/telecommunication line contract, for provision of redundancy.

9. The IT auditor must request for result of previous testing- VERY IMPOTANT-the recovery time achieved during testing must be compared with the expected RTO by the business. In essence every testing must be compared to a measurable objective.

10. Validate the listing/documentation of major vendors and suppliers.

11. Validate the generators are adequately tested.

12. Validate that the critical applications are connected to a UPS

13. Also ensure that Data is backed up according to the defined back-up strategy.

SYSTEMS DEVELOPMENT LIFE CYCLE (SDLC)

AUDITOR'S ROLE IN SDLC.

SDLC is the industry methodology for any project implementation. The industry trend today requires IT Auditors to be part of the Project Implementation Team in order to ensure that IT controls are clearly defined in the Requirement Definition as well as validated during systems design and implementation. The reasoning behind this is to ensure the controls are implemented at the beginning (upfront) rather than detecting weaknesses after implementation or gone life.

PHASES OF SDLC

1. SENIOR MANAGEMENT APPROVAL.

Before the implementation of any project, such implementation must have been approved by the Senior Management. The Auditor must request for the Senior Management approval of the system or application. Some organization refers to this as *Charter Document.*

2. FEASIBILITY STUDIES.

This document is simply the detailed explanation justifying the implementation. There must be *Qualitative and Quantitative* analysis and these must be validated by the Auditor.

Cost Benefit Analysis

Qualitative Benefits: These are benefits that are not quantifiable. They are things of which you can not attach financial value. Examples are;

- Public relations image
- Improved employee morale
- Motivation
- Competitive edge
- Safety and convenience

Quantitative Value to Organization: There must be numeric value.

- Improved productivity (measurable benefit)
- Increased Revenue (there must be a projection)
- Must also consider the cost. Cost is one of the factors to be considered in the decision to build (develop in-house) or buy (already made product) – BUILD or BUY Decision

3. BUSINESS REQUIREMENT DEFINITION.

The requirement definition defines the expectation of the business that should be met by implementing the system or the application. Why are we implementing? If the desire is to implement Oracle Financial, say AP module, the requirement is what you want the application to do for you. Business Requirement is always defined by the business unit or owners.

ORACLE FINANCIAL – Accounts Payable

Business Requirement Definition

AP1.1	**Create AP vendor**
AP1.2	**Periodic Check run**
AP1.3	**Run monthly AP Schedule**
AP1.4	**Create Auto print Checks**
AP1.5	**Transfer Check(s) for approval**

ORACLE FINANCIAL – Accounts Payable

Technical Requirement Definition

AP2.1	Run Oracle Database
AP2.2	Run Microsoft Window
AP2.3	Run SQL Schedule
AP2.4	Run Query for Auto print Checks
AP2.5	

ORACLE FINANCIAL – Accounts Payable

Security Requirement Definition

AP2.1	Ability to capture failed login attempt
AP2.2	Audit log with capability to capture user activities like Add, Delete and Modify.
AP2.3	Identification and Authentication *i.e.* User IDs and Passwords
AP2.4	
AP2.5	

Auditor's Role in Requirement Definition Phase.

- The IT Auditor must ensure that the Business Requirements are dictated by the business unit.
- The IT Auditor must request for a BUYOFF LETTER indicating that the business unit approved of this definition. The buyoff letter is a document that shows the business owner and the name of the business unit representative i.e. Subject Matter Experts (SME) and their names.
- The Auditor must also ensure that the Key IT Controls are defined in the security requirement section of the Business Requirement Definition.

Composition of Project Implementation Team

A typical project implementation team comprises of the following.

I. Project Manager – The PM function is not a technical function, but more focused into managing the implementation team. He reports on the progress of the implementation to the management of the organization. The PMO schedules and coordinates the activities of the team members as well as liaises with the business unit for data, information and meeting requests. (For readers' information, there is a certification for this function called Certified Project Managers)

II. Subject Matter Experts – The SME are the business units representative to the the implementation. They define the Business Requirement as well as signoff/buyoffs on the requirements. They also act as the point of contact for the Developers/Programmers at the design phase of the implementation. Most times, they also help in the Unit Testing.

III. Developers/Programmers – They create the actual designs of the applications based on the defined requirements.

IV. Business Analyst – This function acts as a liaison between the business and IT. They assist the business by interpreting basic requirement into technical terms.

V. System Analyst - They provide assistance to the business providing business related support on the system and application. They review the business need vis-à-vis the business requirement.

VI. The Technical Team - They provide assistance to the team by ensuring a clear, adequate and reasonable definition of the technical requirement. They also assist in the implementation of the hardware and software. Some members of this team include the Database Administrators and LAN Administrators.

VII. IT Auditors – The IT Auditors involvement is to ensure that the interest of the organization and the users in the organization are adequately protected. (See Auditor's Role per phase #3)

4. REQUESTS FOR PROPOSAL (MANDATORY)

In this phase, an RFP will now be sent or publicized for interested vendors to Respond.

S/No	Requirement	Yes?	No?	In Development?
AP1.1	Create AP Vendor			
AP1.2	Periodic Check Run			
AP1.3	Run Monthly AP Schedule			
AP1.4	Create Auto Payment Checks			

YES/NO definition: Yes means the functional requirement is in production OR has been developed to be part of the product

NO means not available and we do not plan to have the functionality i.e. no plans to have it in the pipeline.

IN DEVELOPMENT means there are plans to have the functionality OR in the process of being developed.

Response to RFP

Interested vendors will now provide their responses to the publicized RFP by indicating with a check mark what they currently have in production (Yes column as shown above) and what they do not have (No column) and also what they have in development as indicated in the development column.

Auditor's role in vendors' selection process:

- The criteria for selection must be predefined such as

Cost	- 40%
Business requirement	- 30%
Technical Requirement	- 20%
Financial Stability of the Company	- 10%

Apart from requesting for Management Approval for the project, an Auditor must request and be sure they have the SDLC Methodology in place.

Vendor Demonstration.

After the response by the vendors to the RFPs, the project implementation team selects 2 best vendors that satisfy the requirements per the pre-established selection criteria. These 2 vendors are now requested to come in for the validation (areas marked yes) of existing capabilities of their products.

Every section of the RFPs that the vendors responded to of having current capabilities must be validated.

- The Auditor must ensure that the BR segment is adequately reviewed.
- To also prepare for a vendor demonstration, the Auditor must also ensure that scenarios for validating the requirement is predefined e.g. if what is being implemented is Accounts Payable, AP system, a scenario must be created from creating a vendor through running a check and paying the vendor.

References and Site Visits.

After the vendor demonstration, the project implementation team must determine the performance of the product in a life environment. To accomplish this task, the implementation team will request from the vendor, list of all current customers using their products.

- The IT Auditor must (important) ensure that the Project Implementation team randomly selects the customer's site to visits. The distinction between the demo section and site visit environment is that the demo section does not have live data as well as transaction volume to test full performance of the product.
- The IT Auditor must also ensure that key criteria and requirements for the site visit are well defined. Questions to ask customer are;
    a. Customer's Implementation experience with vendor
    b. Ask about the full performance of the product
    c. What is the reporting capability of the product
    d. Post implementation experience.

Financial Stability of the Vendor

This part of the analysis is done by Senior Management of implementation organization. They put into consideration the financial stability of the company even when all key requirements are met. If the management of the Implementation feels that the vendor is not financially stable (from the review of the audited financial statement, and Senior Management visits to the Company), a decision may be made not to proceed with that vendor.

Selection of the Vendor

The IT Auditor must request for the result of the vendor analysis for validation before the announcement of the finalists. The validations include the followings;

a. Validate the cost provided by each of the vendors and ensure that the vendor with the least cost is marked accordingly.

b. Recount and validate the requirement scoring for each of the vendor

c. Most scorings are performed using excel spreadsheets, ensure the formulae are logical.

5. SIGNING THE CONTRACT.

After the selection of the final vendor, the company will now proceed with signing a contract with the vendor. The IT Auditor's role will ensure the followings:

a. The contract agreement has the involvement of the Legal Department.

b. The responsibilities of the vendor and the implementing company are clearly stated.

c. Liabilities of both parties are clearly stated.

Important: Applications & Systems bugs; the liability of destructive bugs to client data must be clearly defined in the contract

d. Service Level Agreement (Support and Maintenance Agreement): The SLA section of the contract is very important. It defines the responsiveness of the vendor to the application issues based on the level of severity. There are 3 major levels of severity defined in an SLA.

Severity Level	Response Time	Description
Level 1	4hrs	This could be impact affecting more than 20 users
Level 2	24hrs	Impact affecting a small segment of application users
Level 3	48hrs	One or few users impacted

You will always run into SLA in Change Management. Whenever a helpdesk is called, a *Remedy* ticket is opened and from that moment, the *Severity level* and the *Response time* come into play.

e. Support and Maintenance
The IT Auditor must also review the support and maintenance cost section of the contract. The Auditor must validate that every cost must be clearly stated and defined by line item i.e. all the maintenance cost and fees must be itemized. An important area in this regard is the *User License Fee.* The auditor must also ensure that there are no duplicate charges.

6. SYSTEMS DESIGN AND DEVELOPMENT.

This is the phase where the Developer converts the defined requirements into full application

7. TESTING.

This is an important phase of SDLC. The Auditor's role is to ensure that there is a *test plan* and the test plan must include the following:

- Back-out plan
- Test Script
- Corrective Action Plan
- Error reconciliation Process

Types of Testing

- *Regression Testing*

  This is an important testing to ensure that the segment of the test performed has not impacted negatively on the other section of the program.

- *Unit Testing*

  This involves the end users in ensuring that the modules implemented are adequately tested and conforms to the expected requirements. In a Unit Testing, the end users define a scenario and run the scenario thru the application to ensure conformity. The Auditor must ensure the following:

  a. Unit testing errors are documented

  b. Obtain evidence of correction

  c. After every correction, the functionality of the application

  must be retested.

  d. Must obtain the list of the errors and validate the correction of all the errors before Testing is carried out.

  e. There must be a Buyoff Letter or Sign offs by the end users evidencing their satisfaction.

- *Integration Testing*

  This is performed to ensure the full functionality of the product i.e. not just the functionality of the module. You test the functionality and inter-relationship of the product with other function of the system i.e. if the application interfaces with other applications as source of data or data output. The role of an Auditor in this testing is similar to unit testing.

- *Volume Testing*

  Volume Testing tests the ability of the application to handle large volume of transaction.

- *Load Testing*

  Load Testing is a type of testing that mirrors closely the objective of Volume Testing.

- *Stress Testing*

  This measures the response of data call from the database.

- *Parallel Testing.*

  This is the running of newly implemented system alongside of the Legacy System (the system to be replaced)

Data Conversion

The Auditor must ensure that there is a clearly Data Conversion plan with a clearly stated back-out plan. He must also ensure that all required data are converted from the legacy system to the new system. Reconciliation evidence showing that the number of data transferred from the legacy system.

8. GOING LIVE/USER ACCEPTANCE.

At this final stage, the user must sign a document accepting the full functionality of the product. This document is called the User Acceptance Document. After this point, the application is ready to go live.

The General Roles of an IT Auditor

- He must ensure the establishment of project timetable
- He must track and ensure that the milestones in the project timetable are met and all milestones not met must be documented and made known to the project team and management. Not meeting the milestone may impact the Go-live date.
- The auditor must also ensure that implementation cost is being monitored and reported to Management at the end of each milestone. It is more valuable and effective to know in good time if project is highly under funded or under budgeted.

- He must ensure that all the hours of the members of the project implementation is charged to single project number and factored to one single implementation. This must include hours spent by the auditors.

Post Implementation Review

- In a post implementation review, the auditor must validate all sections mentioned above, e.g. Management, Approval, and Feasibility Studies.

BACK UP

Back up is a process whereby files and information that are critic to an organization are stored in two or more places or ways in the event of a loss or disaster, to prevent a total loss of files or information for business continuity.

THE WORD TO REMEMBER IS A TERM:

“No back up no recovery” you can only recover that which was backed up, thing things you did not back up or have a spare stored or kept will be totally loss in the event of trouble.

REASONS WHY YOU MUST DO BACK UPS ARE:

1. Your computer or media will not last for ever, they can crash. For example, your server, your company domain system, your local hard drive, your floppy can go bad or the file stored on it can become corrupted, the same thing goes for your CD disk or and storage device you organization uses to store data.

2. If there is a disaster or a fire out break tomorrow and the city where you have database is destroyed how will you continue business if you don't have back up files or data to do so.

HOW TO DO BACK UP

1. You must have a back offsite in a very far way place from your organization's physical location. A good example is the Iron Mountain, a popular back up company, who store data for other companies at a very far away remote secure sight site.
2. Your company should also have a hot site, a cool site or and a warn site.

HOW TO MAKE BACK UP WORK

1. Your organization must have a back up policy and procedure or plan put in place.
2. You must ensure that every one is in compliance to the defined back up strategy. There is no room for compromise as the company's future may depend on your back ups.

TYPES OF BACK UPS

1. *Total back*: It is also called a full back up, a process where by all the data's on the database are stores or saved, backed up on a tape, to a remote secure saver every week or depending on your company policy and procedure.
2. *Increment back up*: It is also referred to as add on data storage or back up. This is a process where all present transactions are backed up on a daily basis as transactions increment or nothing done by the business from day to day adding they to the full or total back up; until and full back it is done.
3. *Differential back up*: this simple means storing or backing up the difference between the last full back up and today. Don't confuse incremental back up with differential backs they look similar but totally different.

a. Incremental is more, or improvements or any thing done by the business.

b. Differential is anything new, transactions that have not been stored since the last full back up. All or the above is done in a cycle. From week to week every year. You can either do it manually or automatically by scheduling the computer to do it for you.

THINGS THAT ARE CRITICAL TO BACK UPS.

1. Some body or any one must be assigned to monitor backs every morning and very time base on your organization's procedure.
2. Ensure there is always enough paper in back up printers; or space in the saver or hard drive or what ever device or media you use.

YOUR DUTY AS AN IT AUDITOR- BACK UP

1. Validate company policy, procedures and employee compliance.
2. Validate proper tape rotations and Iron mountain tape collection, time and compliance.
3. Validate data retention time or periods as specified the procedure and ensure compliance.
4. Review back up file notifications processes. Is there an alert system put in place, if there is who is to be alerted and is this person or persons in compliance.
5. Ensure that back up options are specified and clearly defined. Either in real time or in batches.

a. Batch back up: done at a given time of the night. Also ensure that back up data's are prioritized in a batch back up, so that the most important or critical data is done first.

b. Real time back up: done side by side along with every transaction every time save tab is clicked.