Workshop on System Audit of Banks – BCP

Workshop on System Audit of Banks

What is Business Continuity Planning (BCP) / Disaster Recovery Plan(DRP) ?

- Preparedness of an organisation to ensure continuity, resumption and recovery of critical business processes.

- Limit the impact of the disaster on people, processes and infrastructure .

- To minimise the operational, financial, legal, reputational and other material consequences.

- A day after the MPSC servers crashed due to a virus, more than 3.5 lakh students who had registered for the April 7 exam, have been told register all over again.

  However, re-registering was not possible as the server continued to crash every time a candidate tried to log in.

- On Monday, Miami County was closed for business and officials said it might not be up until Wednesday.
- Commissioner Josh Francis said the hard drive that failed , shutting the county down, was currently being "recloned." The crash was the county's third this year and shut down a variety of county services.

- **August 19, 2013,** The Core Banking System (CBS) of Indian Overseas Bank(IOB) was affected due to “complex technological malfunction,” restraining the banking services to its customers. This has affected the core banking services and the ATM services of the Bank.

- On 27.01.2014 Lloyds Banking Group faced server failure resulting in taking down thousands of its ATMs and crippling cash cards at the weekend.
- The crash saw thousands of customers unable to withdraw money from their accounts or make payments using debit cards on Sunday afternoon.

- Disaster Recovery Preparedness Benchmark World wide Survey ANNUAL REPORT 2014
- More than one-third (36%)of organizations lost one or more critical applications, VMs, or critical data files for hours at a time over the past year, while nearly one in five companies have lost one or more critical applications over a period of days.
- Reported losses from outages ranged from a few thousand dollars to millions of dollars with nearly 20% indicating losses of more than $50,000 to over $5 million.

The culprits in causing these kind of losses is

- More than 60% - do not have a fully documented DR plan
- 40% admitted - DR plan they currently have did not prove very useful when Called for
- one in four never test their DR plans
- When companies do test their DR plans, the results are most disturbing. More than 65% do not pass their own tests!

- BCP is process and not a project

It should be

- Current –Adaptable to current scenario
- Complete – Covering all aspects say Data, applications, Hardware, Connectivity, people etc.
- Tested – table top walk through to mock drill

- **Regulatory compliances of BCP**
- Basel Committee on E Banking requires
- “Banks should have effective capacity, business continuity and contingency planning processes to help ensure the availability of e-banking systems and services
- The Committee underlines that banks should also ensure that periodic independent internal and/or external audits are conducted about business continuity and contingency planning.

- There are various Indian legislations such as the Information Technology Act, Indian Income Tax act, Central Sales Tax act, State VAT Acts, Services tax act, Central excise act etc. which require data retention for specific number of years.
- The Reserve bank of India provides regular guidelines to cover business continuity and disaster recovery procedures for various types of business operations which are dependent on IT environment. E.g.ATMs, RTGS/NEFT, Mobile Banking etc.

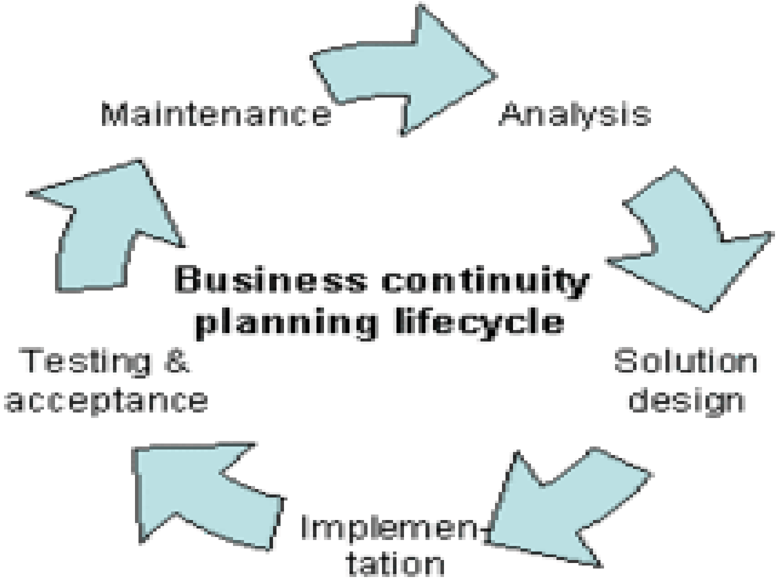
- Sources for BCP
- **COBIT**
- **ISO 22301: Standard on Business Continuity Management**
- 3.3.3 ITIL Information Technology Infrastructure Library (ITIL), a UK body, is a collection of best practices in IT service management www.itil-officialsite.com.

Workshop on System Audit of Banks

Roles, Responsibilities and Organisational structure

- Senior Management
- Co-ordinator
- BCP Team

- Roles and Responsibilities
- Competencies
- Analysis of Approach to training
- Appropriate Training
- Suitable Records



Workshop on System Audit of Banks

Phases of BCP

- *Business Impact Analysis*

Need -> Management Support -> BCP Team -> Work Plan->Initial Report -> Management Approval.

- *Risk Assessment -*

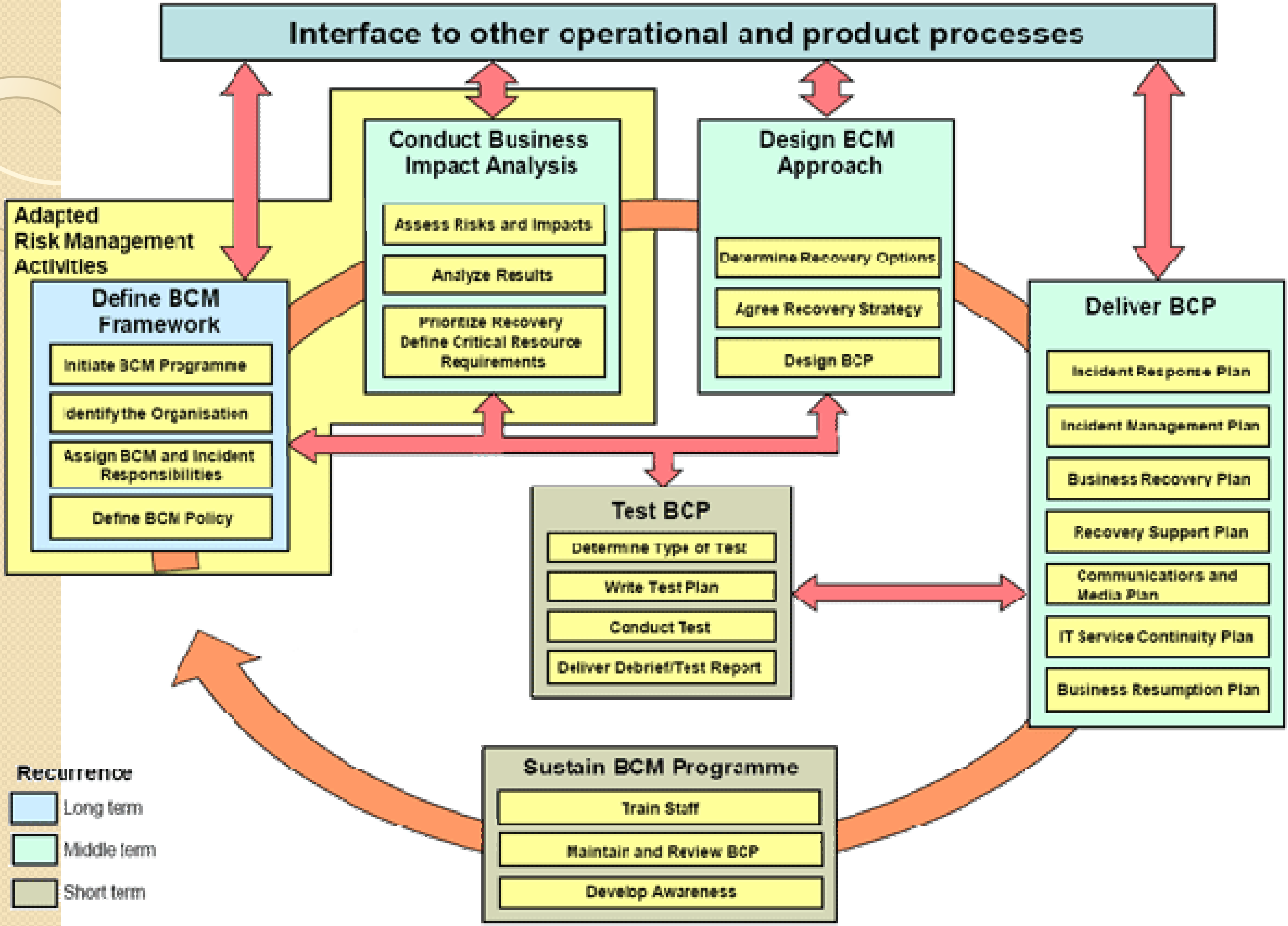
Structured, Attain banks agreed RTOs (Recovery time objectives)/RPOs (Recovery Point Objectives).

- *Determining Choices and Strategy*

Prove Safety, Define Response Action, Arrive at Plan.

- *Development, Testing and Implementation*

Testing, Maintenance, Awareness and Training.



Interface to other operational and product processes

Adapted Risk Management Activities

Define BCM Framework

- Initiate BCM Programme
- identify the Organisation
- Assign BCM and Incident Responsibilities
- Define BCM Policy

Conduct Business Impact Analysis

- Assess Risks and Impacts
- Analyze Results
- Prioritize Recovery Define Critical Resource Requirements

Design BCM Approach

- Determine Recovery Options
- Agree Recovery Strategy
- Design BCP

Deliver BCP

- Incident Response Plan
- Incident Management Plan
- Business Recovery Plan
- Recovery Support Plan
- Communications and Media Plan
- IT Service Continuity Plan
- Business Resumption Plan

Test BCP

- Determine Type of Test
- Write Test Plan
- Conduct Test
- Deliver Debrief/Test Report

Sustain BCM Programme

- Train Staff
- Maintain and Review BCP
- Develop Awareness

Recurrence

- 🟦 Long term
- 🟩 Middle term
- ▨ Short term

Workshop on System Audit of Banks

Key Factors to be considered for BCP Design :

- Identify single points of failure

- Probability of unplanned events
- Security Threats
- Infrastructure and application interdependencies
- Regulatory and compliance requirements
- Failure of Key Third Party Arrangements
- Globalisation and operations in multiple countries

BCP Framework should consider:

- Describe the conditions of plan before its activation.
- Emergency Procedures and liasioning with appropriate authorities
- Identification of processing resourses 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

Workshop on System Audit of Banks

Pandemic Planning:

- epidemics, or outbreaks in humans of infectious diseases that have the ability to spread rapidly over large areas

- much more difficult to determine due to difference in scale and duration

One of the most significant challenges likely from a severe pandemic event will be staffing shortages due to absenteeism.

Banks BCP should provide -

- Preventive programme to reduce the likelyhood of pandemic event
- Document of strategy outlining plan to recover from pandemic wave
- Comprehensive framework of facilities, systems, or procedures
- Impact of customer reactions and the potential demand
- A testing programe to ensure effective practices and capabilities
- Oversight programme to ensure ongoing review and updations

Workshop on System Audit of Banks

RBI Key Recommendations:

- Senior Management is reponsible for prioritising 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

Workshop on System Audit of Banks

Most important industry-wide recommendations are:

- Establishing an industry-wide alarm and crisis organisation
- A website for industry-wide BCP related information for the benefit of constituents
- Reviewing the extent to which the RBI & Individual banks, act on behalf of one another
- Intensifying contacts with the telecommunications and IT Infrastructure providers
- Examining the extent to which institutions can provide reciprocal support
- allowing customers of one bank to use ATM networks of other banks for cash withdrawals
- waiving off penalties to be levied on delay of in-payments of Treasury deals
- making a agreement wherein in need of BCP a participatory Bank will accept request
- conducting a BCP drill on Periodic basis to ensure that the plans and measures are updated
- Industry driven alarm and crisis management team
- Government may declare banking sector including financial markets as critical infrastructure

Workshop on System Audit of Banks

Testing Techniques

- Table Top Testing
- Simulations
- Technical Recovery Testing
- Testing Recovery at an alternate Site
- Tests of Supplier facilities and services
- Complete Rehearsals

Key Considerations forTesting of BCP

- Regular test to ensure that they are up to date and effective.
- Internal Auditors/ System Auditors to check effectiveness of BCP
- Planned BCP drill with critical third party
- Periodic moving of operations to planned fall over or DR site
- Perform tests without moving bank personnel to DR site
- Bank should have unplanned BCP drill

You have to be careful or this may happen.

I WAS JUST WONDERING, DO WE HAVE A DISASTER RECOVERY PLAN?
IT DEPT
© D.Fletcher for CloudTweaks.com

Workshop on System Audit of Banks

Maintenance and Re-assessment of Plans:

-maintained by annual reviews and updates to ensure their continued effectiveness.

-Changes should follow the bank's formal change management process

-BCP, approved by the Board, should be forwarded for perusal to the RBI on an annual basis

Procedural Aspect of BCP:

- BCP should take into account the potential of wide area disasters
- need to put necessary backup sites for critical payment systems
- running critical processes & operations from primary & secondary sites
- prioritising process and alternative location for personnel
- critical processes should be documented to reduce dependency
- Backup/standby personnel should be identified for all critical roles
- relevant portion of the BCP adopted be disseminated to all concerned
- Banks should consider formulating a clear 'Communication Strategy'

Workshop on System Audit of Banks

Infrastructure aspects of BCP

- special attention to availability of basic amenities such as electricity, water and first-aid box

- assigning ownership for each area.

- systems and wireless transmitters on buildings should have backup power

- fallback arrangements be considered & alternative services be carried out in co-ordination with outsiders

- Appropriate updations in case of any new requirement are identified

- not storing critical papers, files, servers in the ground floors

- Fire-proof and water-proof storage areas must for critical documents

- Banks should consider having alternative means of power source

- Banks should consider having an emergency helpline number of key persons

- **Benefits of IT disaster recovery plan**
- The benefits you can obtain from IT disaster recovery plan are as follows –
- Lowering down hazards of delays
- Providing a good sense of safety and security
- Guaranteeing & ensuring the steadfastness of all the standby systems
- Minimizing unnecessarily traumatic and stressful work atmosphere
- Lowering decision making during any sort of disaster
- Providing a good and solid standard for well-testing the plan
- Lowering down the probable legal liabilities

Workshop on System Audit of Banks

Human aspects of BCP:

- People should be an integral part of a BCP.
- BCP awareness programmer be implemented for staff involvement
- Training more than one individual staff for specific critical jobs
- Cross-training employees for critical functions and document-operating procedures
- possibility of enabling work-from-home capabilities and resources

Roll of HR in BCP context

- Crisis Management team
- HR Incident Line
- Exceptional travelling arrangement

Workshop on System Audit of Banks

Technology Aspect of BCP:

- Applications and services in banking system are highly mission critical
- Designing the data centre solution and the corporate network solution

Data Recovery Startegy:

- Recovery Point Objective (**RPO**)–The acceptable latency of data that will be recovered
- Recovery Time Objective (**RTO**)–The acceptable amount of time to restore the function

Common Strategies for Data Protection:

- Backups made to tape and sent off-site at regular intervals
- Backups made to disk on-site and automatically copied to off-site disk
- Replication of data to an off-site location
- Availability of systems that keep both data and system replicated,
- Use an outsourced disaster recovery provider
    - Local mirrors of systems or data
    - Surge protectors—to minimize the effect of power surges
    - Uninterrupted power supply (UPS) or backup generator
    - Fire preventions and Anti Virus software and security measures.

Workshop on System Audit of Banks

Issues in choosing a backup site and implementing a DC/DR

Backup Sites :

- Cold Sites : most inexpensive
- Warm Sites : a compromise between hot and cold
- Hot Sites : a duplicate of the original site

- Solution architectures are not identical for all the applications & services
- servers, network devices etc have to be identical at all times
- Periodic checks on integrity between DC&DR are mandatory
- Solutions to be defined in RTO & RPO parameter
- RTO and RPO is more to follow the industry practice
- Technology operations processes need to formally included into the IT Continuity Plan.
- Banks may need to consider near site DR architecture

Workshop on System Audit of Banks

Issues/challenges in implementing DC/DR by Banks

- Continuity & recovery aspects are impacting IT strategy & cost implications are challenging IT budgets.

- Time window for recovery is shrinking in face of the demand for 24 / 365 operations

- Establish the justification for continuity for specific IT and telecommunication services

- Regular assessment of the security health of the organisation and proactive steps to detect and fix any vulnerability

- Rigorous self-assessment of security measures
- Random Security Preparedness
- Telecommunications issues
- telecommunications diversity components
- Monitor service relationship with telecommunication providers
- Outsourcing risks

Workshop on System Audit of Banks

CAs can be involved in any/all areas of BCP implementation or review. These areas could be pertaining to:

- a. Risk Assessment
- b. Business Impact Assessment
- c. Disaster Recovery Strategy Selection
- d. Business Continuity Plan Development
- e. Fast-track Business Continuity Development
- f. BCP / DRP Audit, Review and Health-check Services
- g. Development and Management of BCP / DRP Exercises and Rehearsals
- h. Media Management for Crisis Scenarios
- i. Business Continuity Training