Business continuity and disaster recovery planning

Business continuity plan and Disaster recovery plan is activity to help organisation prepare for disruptive events and it is essential to consider the potential impact of disaster and understand the underlying risks. In this my research, I explore business continuity planning and Disaster recovery planning and its importance in support of operation and establish to manage availability of critical process in the event of interruption.

Introduction

Business continuity planning (BCP) and disaster recovery planning (DRP) is a vital role in the organisation. These plans are basic to the well being of an organisation and anticipated to make sure stability in the face of unexpected or difficult situation. Planning for these conditions is not always directly ahead neither identifies appropriate cause of information, products, and services. These tasks are also challenging and build of the plan itself. These plans has provision of information and guidance to identify the suitable tools and used in the right time.

Organisation has created this plan itself and necessary to consider the possible impacts of disaster and recognize the fundamental risks and build BCP and DRP. “ Following these activities the plan itself must be constructed – no small task. This itself must then be maintained, tested and audited to ensure that it remains appropriate to the needs of the organization”. These plans are calculated to consider all these issues and find the software to assist with BIA and risk analysis along with link the tools to help to create, maintain, and audit the plan itself. (BCP, 2004)

BCP and DRP are significant to the clear and continue operation of all type of business. BCP involves developing a reaction strategy for organisation respond to disaster. Disaster occurs through power failure, accident, natural, IT system Clash, insider attacks, hacking, terrorism etc. (Barney, 2010) BCP check how organisation will take to maintain its operations in emergency and identify potential disasters or emergencies, verify how intend to minimize the risk of disaster occur, creating plan reaction, test BCP regularly. These strategies assume increase importance as organisation become increasingly reliant on technology to do business. " As companies place more emphasis on IT and communications services to support their customer communications and transactions, or to help manage supply chains. They become less tolerant of information and service loss as a consequence of disasters". (4service, 2010)

This research work deal with business continuity plan will keep business up and running through interruption of any kind of disaster and support of operations and establish to manage availability of critical process.

1. 1 Identify and critically explore business continuity and its importance in business environment, distinguish between business continuity (BC) and disaster recovery (DR) planning.

Business Continuity

Business continuity planning identifies the exposure of organisation internal and external threats and creates information assets to provide useful prevention and recovery for the organisation and maintain economical benefit and value of system integrity and perform policies, procedures, processes, and plans to certify the continue function in the organisation.

Business continuity plan take to prevent disruption of essential services and restore function as rapidly and smoothly. Business continuity planning develops the business ability to respond to such disruption and resume operations in order to meet business significant necessity.

BCP Importance in business environment

Business continuity is a process build up to counter system failure. If IT system fails, its major impact on the whole business consequently organisation should take dynamic interest in start business continuity plan for IT systems. A business continuity plan for your IT systems should include arrangements for providing:

Facilities and services to enable the business to continue to function;

The critical IT applications and infrastructure necessary to support the recovery of business processes. (Varney, 2010)

It is important the BCP plan is clear and brief to certify to every user read it and build available to all staff responsible for any part of it and it is start of ongoing commitment and also update the business continuity plan. (Varney, 2010)

Distinguish between BCP and DRP

Business Continuity Planning

Disaster Recovery Planning

Business Continuity is Proactive;

Disaster Recovery is Reactive;

BCP focus is to avoid or mitigate the impact of the risk;

DRP focus is to pick-up the part and re-establish the organisation to business following risk occurs;

BCP has as its scope the entire organisation with critical goal being recovery of mission-critical/ middle business functions to make sure the endurance of the organisation;

DRP is normally limited in scope to set of classify IT system and infrastructure with goal being entire recovery of the system and infrastructure within a timeframe and minimum data loss;

Business functions to recover in BCP extend beyond IT system;

DRP might exclude non-IT business units; (Nickolett, 2001)

BCP fill up the gap between the disruption occurrence and recovery going on.

DRP engage a breakdown, loss of the systems, people, and facilities. The disruption can impact any or all of these key business inputs.

1. 2 Evaluate and explain some business worst case scenarios for risk assessment, assess different types of organisational assets.

Worst case scenarios for risk assessment

There are many worst cases scenarios for risk assessment some are as below:

Information data lost – Disaster can damage the database and organisation loss confidential data such as staff, customer, vender details and other sensitive information;

Information system failure – There are many worst cases in information system failure such as overlooked, quality of project planning, use of management tools, object-oriented system development, use software engineering tools and system essential services can stop for time being etc. (Megaessays 2010)

Information asset lost – Due to the weak security measures Information assets can damage from natural disaster and internal activities in the organisation;

Natural Disaster – Natural disaster are unexpected and it is impossible to fully recover the damage caused by the disaster but it is possible to minimise the potential risk by developing BCP/DRP. (Banger, 2010)

Power failure – Sometime disruption of power supply or power failure can stop work, services failure, breakdown etc. It can effect in the business.

There is one real example of the worst case scenarios for risk assessment is Midmarket CIOs. This company is on the seventh floor of a building but one day in the next office door the water filter cracked in the office kitchen and sending water flow on the floor and under the wall into facilities. “ Although critical servers remained dry, the flood ruined equipment that was on the office floor, including 10 surge protectors, six uninterruptible power supplies, six power bricks and one PC. While things were drying out and a length of wallboard was replaced”. CIOs implemented DRP to ability for total different incident because floods, fires, power failures and pandemic flu can occur. CIOs take step back and start with risk assessment of all the risks business faces and using risk management tools to calculate worst case scenarios in IT and effect potential loss will have on the business. (Midmarket, 2009)

Different types of organization assets

There are following different types of organisation assets to protect in BCP and DRP are:

Desktop workstation, Laptops, Servers, Printers, Scanners, Firewalls, Routers, Switches, Memory devices etc;

Licences Software CDs such as windows, Antivirus, MS Office, software tools and support, other operating system etc;

Database, websites, Photo Copiers, Fax Machines, Telephone System, Multifunction machines etc;

Paper file records like asset register, paper files, data, books, government legislation, policies and procedures, customer data and sensitive data etc;

Electronic records such as emails, organisation shared drives and personal drives, DVDs, CDs, Memory sticks etc;

Maps, drawers, chairs, desks, cabinets, etc;

Qualified staffs, Record management, etc;

Machines, Plants, building, fire extinguishers etc.

1. 3 Explain critically disaster recovery business case, list down and appraise required documentation for BCP and DRP.

Disaster recovery business case

The most critical parts of any IT plan explain the business case and assess of the potential risks to the organisation. There are eight following project steps in Disaster Recovery Planning in business are:

Step-1: Project introduction – Set the objectives of the DRP initiation, define the scope, develop, schedule and identify the risk to the project;

Step-2: Assess of Disaster Recovery – Assess of location, building composition, computing environment, physical plant security, installed security devices, access control system, software, personal, backup, and operating practices;

Step-3: Business Impact Analysis for IT – Analysis of all part of business units to support by the IT areas should assume to identify the system and its functions to continuation of the business and the time limit;

Step-4: Define of requirements – All requirements must be defined and detailed;

Step-5: Plan the project – project planning will define the project to be executed and its objectives will develop the DRP;

Step-6: Execute the project – Project must proceed to practices of project management and identify the methods of mitigating the risk will execute;

Step-7: BCP combination – DRP needs to combine back in to the organisation’s business continuity efforts;

Step-8: ongoing maintenance and combination – Ongoing maintenance and testing efforts require keeping the plan up to date and processes to identify and mitigate future risks.

Required Documentation for BCP and DRP

There are following necessary document for Business Continuity Plan and Disaster Recovery Plan in the organisation to make a best pan for long run business as follows:

Organisation Chart [explain names and designation];

If existing BRP and DRP and their terms explain in the documentations;

Scope of BCP and DRP, Procedures and control documents;

The report of Business impact analysis and risk assessment report;

Staff, list of vendors, list of emergency services, advisor contact details;

Details of IT system and communication system specification include maintenance agreements;

Existing evacuation procedure, Health & safety procedures, fire regulations, operations and administrative procedures;

Details organisation asset, information assets, and IT records;

Relevant organisation regulations, guidelines and insurance information.

Details any other documents for the support of BCP and DRP. (Yourwindow, 2010)

1. 4 Demonstrate and explore pragmatic approach towards project planning and initiation, describe how to evaluate risk and control in terms of BCP/DRP.

Pragmatic approach towards project planning and initiation

A pragmatic approach towards project planning needs to be comprehensive and cover all relevant aspects and factors in BCP and DRP. There are some BCP and DRP following steps as follows:

Business continuity plan

Step-1: Identify strategy objective through performing needs and create outline for strategy performance;

Step-2: Establish the business value and identify recovery objectives through data risk and recovery time outline;

Step-3: Technology will equivalent for data protection along with backup, disaster recovery etc;

Step-4: Identify infrastructure and organisational plan;

Step-5: Implement technologies and inform key personnel as to which business processes are impacted;

Step-6: Test the documented plan continuously;

Step-7: Calculate and authenticate test results comparative to the plan's objectives;

Step-8: Implement required development and priority as a result of continue testing and evaluation;

Step-9: continue review and enhance the BRP to replicate organisation change and added new technologies;

Step-10: Ensure the entire process continuously. (Miller, 2007)

Disaster Recovery Plan

There are following steps to DRP involves:

Outline DRP team with senior executives from IT department with specific responsibilities;

Perform Business impact analysis and Risk analysis for business assets, threats and impacts the risk can tolerate need to be determined;

Develop recovery strategies – IT security measures like backup etc;

Implementation, testing and training – the employee must be trained in the disaster recovery procedures and testing capabilities;

Need to carry out periodic audit, review and drills of BCP and DRP;

Types of disaster which need to be addressed;

The essential business processes and activities which are needy on IT;

The data and application software needs to be recovered and restored in case of disaster and IT services need to continue function of the event;

The IT infrastructure need to host the data and application software;

DRP arrange strategies and implementation such as backup and protection facility;

Challenges and emerging threats.(Periasamy, 2007)

Bottom of Form

Evaluate risk and control in terms of BCP/DRP

Evaluate the risk is vital activity in the organisation. There are major threats against business continuity plan and disaster recovery plan are:

Risk or threats

Natural disaster – Fire, flood, earthquake, volcanic eruption, tornadoes, cyclone, heat wave water disaster etc;

Information system threats – software failure, loss of information and data, system failure, cyber crime, multiple machine failure, capacity overload, network failure, etc;

Planned activities – war, terrorist attacks, hacking, breach the network and database, data theft, unauthorised modification of content, phishing etc;

Lack of utilities – power failure, electricity fail, air conditioning failure etc;

Other vital threats – Internal violence and dispute, legislative violation, labour strike, other strike, etc.

Controls

Classify the risk (High, medium, low) it will be easy to describe the risk;

Control must be according to the risk like backup system, data, building etc;

Proper monitoring the risks and threats;

Risk must be clear and explain;

Risk evaluations identify the threats which help to control it.

1. 5 Critically explain business impact analysis (BIA) activity and describe how to execute it, assess emergency response and operations during period of IT disruption.

Business impact analysis activity

Business impact analysis is an important part of any organisation business continuance plan. BIA is a logical process to identify business significant systems and activity as sign to any business continuity, disaster recovery, or emergency planning effort and reveal vulnerabilities and planning component to develop strategies for minimizing risk. One or more risk identifies causes of the loss of the application, systems, tools or other resource upon that activity is dependent. BIA identifies cost related to failures and it report measure the importance of business components and recommend suitable fund allocation for measures to protect them. (Miller, 2010)

How to execute BIA

Business impact analysis execute following guideline to allow organisation are as follows:

Effectively identify the proper organisational impact of any unexpected disruption of essential information processing systems such as fire, earthquake, theft etc;

Identify threats sources and significant vulnerabilities which can lead to unexpected outages / service disruption;

Execute suitable protect to reduce the likelihood and consequences should identify threats happen;

Increase cost effective and suitable contingency plans and important component disaster recovery / business continuity planning.

Emergency response and operations during the period of IT disruption

In case of IT disruption or failure, every organisation has quick emergency response plan to stop and control any damages. Emergency response facility is available in every organisation and DRP team identify the threats of failures. Some of the major elements of emergency response plan as below:

Emergency response plan and procedure;

Command, control and emergency operations centre;

Emergency reporting procedure, employee evacuation plans, health and safety, security plans;

Identify the disaster in IT;

Personnel protection, incident control, effect assessment, choose maximum action etc;

Emergency response components such as incident preparation, emergency action, facility stabilization, damage mitigation, and testing procedures etc. (Hui, Z, 2010)

Above elements help to stop the disaster and resume as soon as possible in every organisation.

1. 6 Explore and appraising different developing and implementing business continuity strategies used by most organisations.

Developing and implementing business continuity strategies

The business continuity strategies have five key stages in developing and implementing used by organisation as follows:

Understand the business

Project initiation and create a management structure to build up and carry out the plan;

Identify the risk and perform risk evaluation and control;

Establish your business impact analysis process and identify the impact of any failures.

Business continuity management

Develop business continuity strategy and identify the areas and focus on the critical operating requirement of the business;

Develop a process level and documented structure stating how significant process will be restarted subsequent failures.

Business continuity response

Establish a crisis management process to respond to incidents;

Focus on overall business continuity strategy;

Put in place business unit plans for every department.

Develop business continuity management culture

Awareness and training plans;

Review the effectiveness of awareness training plans.

Exercising, maintenance and audit

Test the business continuity plans and technical aspects;

Maintain the plan and ensure that the documentation remains accurate and reflects any changes inside or outside the business;

Regularly audit plans. (Business link, 2010)

Conclusion

I conclude that Business continuity plan and Disaster recovery plan play vital role in every organisation and BCP is ideal strategy to safe business away from a complete disaster because every organisation faces different type of risk and potential disaster and it is an essential tool to allow minimizing the risk and also continuously helps to stop IT disruption and services. BCP involve IT as the main component because every business relies on computer system and its existence can be equalised to the business itself.

Recommendation

BCP should recognize organisational structure including incident and risk assessment cover all business activities and document strategy for recovery of the organisation all main areas of the business process and DRP team should deal with disaster recovery phases to complete and minimize the disaster as soon as possible. I recommend following key points related to BCP and DRP plan to become a successful plan in the organisation as below:

Employee training timely;

Perform schedule test and evaluation of test result;

Implement of test plan updates;

Conduct crisis management exercises;

Perform business impact analysis timely;

Top management support every time;