

BUSINESS CONTINUITY PLANNING AND DISASTER RECOVERY PLANNING

Question 1

Discuss the objectives and goals of Business Continuity planning. (5 Marks) (Nov 2008)

Answer

Objectives and Goals of Business Continuity Planning: The primary objective of a business continuity planning is to enable an organization to survive in a disaster and to re-establish normal business operations. In order to survive, the organization must assure that critical operations can resume normal processing within a reasonable time frame. The key objectives of the contingency plan should be to:

- (i) provide for the safety and well-being of people on the premises at the time of disaster;
- (ii) continue critical business operations;
- (iii) minimise the duration of a serious disruption to operations and resources (both information processing and other resources);
- (iv) minimise immediate damage and losses;
- (v) establish management succession and emergency powers;
- (vi) facilitate effective co-ordination of recovery tasks;
- (vii) reduce the complexity of the recovery effort; and
- (viii) identify critical lines of business and supporting functions.

Therefore, the goals of the business continuity plan should be to:

- (i) identify weaknesses and implement a disaster prevention program;
- (ii) minimise the duration of a serious disruption to business operations;
- (iii) facilitate effective co-ordination of recovery tasks; and
- (iv) reduce the complexity of the recovery effort

Question 2

Describe the methodology of developing a Business Continuity Plan. (5 Marks) (Nov 2008)

Answer

The methodology for developing a business continuity plan can be sub-divided into eight different phases. The extent of applicability of each of the phases has to be tailored to the respective organisation. The methodology emphasises on the following:

- (i) Providing management with a comprehensive understanding of the total efforts required to develop and maintain an effective recovery plan;
- (ii) Obtaining commitment from appropriate management to support and participate in the effort;
- (iii) Defining recovery requirements from the perspective of business functions;
- (iv) Documenting the impact of an extended loss to operations and key business functions;
- (v) Focusing appropriately on disaster prevention and impact minimisation, as well as orderly recovery;
- (vi) Selecting business continuity teams that ensure the proper balance required for plan development;
- (vii) Developing a business continuity plan that is understandable, easy to use and maintain; and
- (viii) Defining how business continuity considerations must be integrated into ongoing business planning and system development processes in order that the plan remains viable over time.

Question 3

What do you understand by the term Disaster? What procedural plan do you suggest for disaster recovery? (10 Marks) (Nov 2008)

Answer

The term disaster can be defined as an incident which jeopardizes business operations and/or human life. It could be due to sabotage (human) or natural. Following is the procedural plans for disaster recovery.

Disaster Recovery Procedural Plan: Normally disaster recovery procedural plan is made when the system is normally working. After visualizing the disaster the action to be taken by different people of the organization are to be documented. This recovery and planning document may include the following areas:

- (i) The conditions for activating the plans, which describe the process to be followed before each plan, are activated.
- (ii) Emergency procedures, which describe the actions to be taken following an incident which jeopardises business operations and/or human life. This should include arrangements for public relations management and for effective liaison with appropriate public authorities e.g. police, fire, services and local government.
- (iii) Fallback procedures which describe the actions to be taken to move essential business activities or support services to alternate temporary locations, to bring business process back into operation in the required time-scale.
- (iv) Resumption procedures, which describe the actions to be taken to return to normal business operations.
- (v) A maintenance schedule, which specifies how and when the plan will be tested, and the process for maintaining the plan.
- (vi) Awareness and education activities, which are designed to create an understanding of the business continuity, process and ensure that the business continues to be effective.
- (vii) The responsibilities of individuals describing who is responsible for executing which component of the plan. Alternatives should be nominated as required.
- (viii) Contingency plan document distribution list.
- (ix) Detailed description of the purpose and scope of the plan.
- (x) Contingency plan testing and recovery procedure.
- (xi) List of vendors doing business with the organization, their contact numbers and address for emergency purposes.
- (xii) Checklist for inventory taking and updating the contingency plan on a regular basis.
- (xiii) List of phone numbers of employees in the event of an emergency.
- (xiv) Emergency phone list for fire, police, hardware, software, suppliers, customers, back-up location, etc.
- (xv) Medical procedure to be followed in case of injury.
- (xvi) Back-up location contractual agreement, correspondences.
- (xvii) Insurance papers and claim forms.
- (xviii) Primary computer centre hardware, software, peripheral equipment and software configuration.
- (xix) Location of data and program files, data dictionary, documentation manuals, source and object codes and back-up media.
- (xx) Alternate manual procedures to be followed such as preparation of invoices.

(xxi) Names of employees trained for emergency situation, first aid and life saving techniques.

(xxii) Details of airlines, hotels and transport arrangements.

Question 4

Briefly explain the various types of system's back-up for the system and data together.

(5 Marks) (Nov 2008)

Answer

Types of system's Back-ups: When the back-ups are taken of the system and data together, they are called total system's back-up. System back-up may be a full back-up, an incremental back-up or a differential back-up.

- (i) *Full Backup:* Every backup generation contains every file in the backup set. However, the amount of time and space such a backup takes prevents it from being a realistic proposition for backing up a large amount of data. This is the simplest form of backup with a single restoring session for restoring all backed-up files.
- (ii) *Differential Backup:* It contains all the files that have changed since the last full backup. This is in contrast to incremental backup generation, which holds all the files that were modified since the last full or incremental backup. It is faster and more economical in using the backup space, as only the files that have changed since the last full backup are saved.
- (iii) *Incremental Backup:* Only the files that have changed since the last full backup / differential backup / or incremental backup are saved. This is the most economical method, as only the files that changed since the last backup are backed up. This saves a lot of backup time and space. Normally, it is difficult to restore as you have to start with recovering the last full backup, and then recovering from every incremental backup taken since.
- (iv) *Mirror back-up:* It is identical to a full backup, with the exception that the files are not compressed in zip files and they can not be protected with a password. A mirror backup is most frequently used to create an exact copy of the backup data.

Question 5

As a system auditor, what control measures will you check to minimize threats, risks and exposures in a computerized system?

(10 Marks) (Jun 2009)

Answer

To minimize threats to the confidentiality, integrity, and availability, of data and computer systems and for successful business continuity, the system auditor should evaluate potential

threats to computer systems. Discussed hereunder are various control measures that will be checked by him to minimize threats, risks and exposures in a computerized system:

- (i) *Lack of integrity* : Control measures to ensure integrity include implementation of security policies, procedures and standards, use of encryption techniques and digital signatures, inclusion of data validation, editing, and reconciliation techniques for inputs, processes and outputs, updated antivirus software, division of job and layered control to prevent impersonation, use of disk repair utility, implementation of user identification, authentication and access control techniques, backup of system and data, security awareness programs and training of employees, installation of audit trails, audit of adequacy of data integrity.
- (ii) *Lack of confidentiality*: Control measures to ensure confidentiality include use of encryption techniques and digital signatures, implementation of a system of accountability by logging and journaling system activity, development of a security policy procedure and standard, employee awareness and training, requiring employees to sign a non-disclosure undertaking, implementation of physical and logical access controls, use of passwords and other authentication techniques, establishment of a documentation and distribution schedule, secure storage of important media and data files, installation of audit trails, and audit of confidentiality of data.
- (iii) *Lack of system availability*: Control measures to ensure availability include implementation of software configuration controls, a fault tolerant hardware and software for continuous usage and an asset management software to control inventory of hardware and software, insurance coverage, system backup procedure to be implemented, implementation of physical and logical access controls, use of passwords and other authentication techniques, incident logging and report procedure, backup power supply, updated antivirus software, security awareness programmes and training of employees, installation of audit trails, audit of adequacy of availability safeguards.
- (iv) *Unauthorized users attempt to gain access to the system and system resources*: Control measures to stop unauthorized users to gain access to system and system resources include identification and authentication mechanism such as passwords, biometric recognition devices, tokens, logical and physical access controls, smart cards, disallowing the sharing of passwords, use of encryption and checksum, display of warning messages and regular audit programs.

Data transmitted over a public or shared network may be intercepted by an unauthorized user, security breaches may occur due to improper use or bypass of available security features, strong identification and authentication mechanisms such as biometric, tokens, layered system access controls, documentation procedures, quality assurance controls and auditing.

- (v) *Hostile software e.g. virus, worm, Trojan horses, etc.*: Establishment of policies regarding sharing and external software usage, updated anti-virus software with detection, identification and removal tools, use of diskless PCs and workstations, installation of

intrusion detection tools and network filter tools such as firewalls, use of checksums, cryptographic checksums and error detection tools for sensitive data, installation of change detection tools, protection with permissions required for the 'write' function.

- (vi) *Disgruntled employees*: Control measures to include installation of physical and logical access controls, logging and notification of unsuccessful logins, use of disconnect feature on multiple unsuccessful logins, protection of modem and network devices, installation of one time use only passwords, security awareness programs and training of employees, application of motivation theories, job enrichment and job rotation.
- (vii) *Hackers and computer crimes*: Control measures to include installation of firewall and intrusion detection systems, change of passwords frequently, installation of one time use passwords, discontinuance of use of installed and vendor installed passwords, use of encryption techniques while storage and transmission of data, use of digital signatures, security of modem lines with dial back modems, use of message authentication code mechanisms, installation of programs that control change procedures, and prevent unauthorized changes to programs, installation of logging feature and audit trails for sensitive information.
- (viii) *Terrorism and industrial espionage*: Control measures to include usage of traffic padding and flooding techniques to confuse intruders, use of encryption during program and data storage, use of network configuration controls, implementation of security labels on sensitive files, usage of real-time user identification to detect masquerading, installation of intrusion detection programs.

Question 6

What are the audit tools and techniques used by a system auditor to ensure that disaster recovery plan is in order? Briefly explain them.
(5 Marks) (Jun 2009)

Answer

Audit tools and techniques used by a system auditor to ensure that the disaster recovery plan is in order, are briefly discussed below:

The best audit tool and technique is a periodic simulation of a disaster. Other audit techniques would include observations, interviews, checklists, inquiries, meetings, questionnaires and documentation reviews. These are categorized as follows:

- (i) *Automated tools*: They make it possible to review large computer systems for a variety of flaws in a short time period. They can be used to find threats and vulnerabilities such as weak access controls, weak passwords, and lack of integrity of the system software.
- (ii) *Internal Control auditing*: This includes inquiry, observation and testing. The process can detect illegal acts, errors, irregularities or lack of compliance for laws and regulations.
- (iii) *Disaster and Security Checklists*: These checklists are used to audit the system. The checklists should be based upon disaster recovery policies and practices, which form the

baseline. Checklists can also be used to verify changes to the system from contingency point of view.

(iv) *Penetration Testing*: It is used to locate vulnerabilities to the system.

Question 7

What analysis should be done for understanding the degree of potential loss (such as reputation damage, regulation effects) of an organization? Enumerate the tasks to be undertaken in this analysis. In what ways the information can be obtained for this analysis?

(10 Marks) (Nov 2009)

Answer

Business Impact Analysis (BIA) should be done for assessing the potential impacts resulting from various events or incidents. It is intended to help in understanding the degree of potential loss which could occur. It covers not only financial loss but also other losses due to reputation damage, regulatory effects, etc.

For BIA, the following tasks are to be undertaken:

- Identify organizational risks, and to minimize potential threats that may lead to a disaster,
- Identify critical business processes,
- Identify and quantify threats/ risks to critical business processes both in terms of outage and financial impact.
- Identify dependencies and interdependencies of critical business processes and the order in which they must be restored.
- Identify the maximum allowable downtime for each business processes,
- Identify the type and the quantity of resources required for recovery, and
- Determine the impact to the organisation in the event of a disaster.

The information for this analysis can be obtained in many ways, including:

- Questionnaires,
- Workshops,
- Interviews, and
- Examination of documents.

Question 8

A company has decided to outsource a third party site for its alternate back-up and recovery process. What are the issues to be considered by the security administrator while drafting the contract?
(5 Marks) (May 2010)

Answer

If a third party site is to be used for backup and recovery purposes, security administrators must ensure that a contract is written to cover the following issues :

- How soon the site will be made available subsequent to a disaster,
- The number of organizations that will be allowed to use the site concurrently in the event of a disaster,
- The priority to be given to concurrent users of the site in the event of a common disaster,
- The period during which the site can be used,
- The conditions under which the site can be used,
- The facilities and services the site provider agrees to make available, and
- What controls will be in place and working at the off-site facility.

The above are the main issues that should be covered while drafting a contract. These issues are often poorly specified in reciprocal agreements. Moreover, they can be difficult to enforce under a reciprocal agreement because of the informal nature of the agreement.

Question 9

"Technology risk assessment needs to be a mandatory requirement for project to identify single point's failures." – Justify.
(4 Marks) (Nov 2010)

Answer

Single point of failures have increased due to the continued growth in the complexity in the organization's IS environment. Technology risk assessment is a mandatory requirement to identify single point failures because of the following benefits:

- (i) A business-driven process to identify, quantify and manage risks while detailing failure, suggestions for improvement in technical delivery.
- (ii) A framework that governs technical choice and delivery processes with cyclic checkpoints during the project life-cycle.
- (iii) Interpretation and communication of potential risk impact and where appropriate, risk reduction to a perceived acceptable level.

- (iv) Implementation of strict disciplines for active risk management during the project life cycle.

The technology risk assessment ensures that proactive management of risks occurs and that no single point of failure is inadvertently built into the overall architecture.

Question 10

Describe the benefits of performing a technology risk assessment. (4 Marks) (May 2011)

Answer

Benefits of performing a technology risk assessment are given as follows:

- To have a business driven process to identify, quantify, and manage risks while detailing future suggestions for improvement in technical delivery;
- To have a framework that governs technical choice and delivery processes with cyclic checkpoints during the project lifecycle;
- Interpretation and communication of potential risk impact and where appropriate, risk reduction to a perceived acceptable level; and
- Implementation of strict disciplines for active risk management during the project lifecycle.

The technology risk assessment needs to a mandatory requirement for all projects to ensure that proactive management of risks occurs and that no single point of failure is in advertently built into the overall architecture.

Question 11

Discuss the various backup options considered by a security administrator when arranging alternate processing facility. (4 Marks) (May 2011)

Answer

Security administrators should consider the following backup options while arranging alternate processing facility:

- **Cold site:** If an organization can tolerate some down time, cold site backup might be appropriate. A cold site has all the facilities needed to install a mainframe system, raised floors, air conditioning, power, communication lines, and so on. An organization can establish its own cold site facility or enter into an agreement with another organization to provide a cold site facility.
- **Hot site:** If fast recovery is critical, an organization might need hot site backup. All hardware and operations facilities will be available at the host site. In some cases, software, data and supplies might also be stored there. A hot site is expensive to

maintain. They are usually shared with other organizations that have hot site needs.

- **Warm site:** It provides an intermediate level of backup. It has all cold site facilities in addition with hardware that might be difficult to obtain or install. For example, a warm site might contain selected peripheral equipment plus a small mainframe with sufficient power to handle critical applications in the short run.
- **Reciprocal agreement:** Two or more organizations might agree to provide backup facilities to each other in the event of one suffering a disaster. This backup option is relatively cheap, but each participant must maintain sufficient capacity to operate another's critical system.