Question 1

Explain the fundamental difference between business continuity planning (BCP) and disaster recovery planning (DRP).

Student should consult lecture slides on BCP to recognise that DRP is a sub-component of BCP (BCP consists of: BIA, COOP + DRP, Testing, and Maintenance). BCP is a process designed to reduce the organizations business risk arising from and unexpected disruption of the critical functions/operations (manual or automated) necessary for the survival of the organization, whilst DRP typically details the process IT personal still follow to restore the computer system and the operational facilities after a disaster

.

Question 2

What is business impact analysis (BIA), and what is it used for?

A business impact analysis and a systematic process to determine and evaluate the protection of facts of an action to critical business operations. As a result of a disaster actually did have images, and it is used for identifying critical activities, identify resources to support this activity, evaluate the impact of using to perform these activities and identify priorities and determine recovery criticality.

The BIA is the first phase of BCP. A crucial component of the initial planning stages, it serves as an investigation and assessment of the impact that various event can have on the organization. It includes

Determine core business processes and recover criticality

Identify resource requirements

Identify recover priorities for system resources

Question 3

What is the fundamental difference between BIA and risk assessment?

Risk management focus on identifying threats

Bia assume that these controls have failed, bypassed or ineffective , these

Therefore addresses worst case scenarios

Risk management focuses on identifying threats, vulnerabilities, and attacks in order to determine controls that can protect data. BIA on the other hand assumes that these controls have FAILED/BY-PASSED/INEFFECTIVE, and the attacks have been successful. BIA therefore addresses worst-case scenarios.

Question 4

The comprehensive approach to emergency or disaster management typically consists of four phases: Prevention, Preparedness, Response, and Recovery (PPRR). Which phase does Business Impact Analysis (BIA) belong to? Describe two (2) examples of critical activities of a typical software firm that need to be established as part of business impact analysis.

Preparedness.

Software frim sim to manufacturing firm,

Securing contracts w clients

Developing software

Delivering and developing software products

BIA belongs to: Preparedness

A software firm is similar to manufacturing firm as in the QLD BCP Guide, so example can be found similarly as follows

Securing contracts with clients

Developing software

Delivering and supporting developed software products

Question 5

Explain why it is important for large organisations to have a proper BCP in place? What is the implication if a lack of BCP is found?

Legal and regulatory req: many industries may find themselves bound by federal, state and local laws or regulations that require them to implement various degrees of Business Continuity Planning. For example, the officers and directors of publicly traded firms have a fiduciary responsibility to exercise due diligence in the execution of their business continuity duties. In other circumstances, the requirements(and consequence of failure) might be more severe. Emergency services, such as police, fire, and emergency medical operations, have a responsibility to the community to continue operations in the event of a disaster. Indeed, their services become even more critical in an emergency when public safety is threatened. Failure on their part to implement a solid BCP could result in the loss of life and/or property and the decreased confidence of the population in their government.

In many countries, financial institutions, such as banks, brokerages,and the firms that process their data, are governed by strict government and international banking a d securities regulations designed to facilitate their continued operation to ensure the viability of the national economy. Why pharmaceutical manufacturers must produce products in less-than-optimal circumstances following a disaster, they are required to certify the purity of their products to government regulators. There are countless other examples of industries that are required to continue operating in the event of an emergency by various laws and regulations.

Var deg of bus continuity planning

Eg. the officers and directors o

Due diligence in the business continuity

Cons

Emergency services such as

Their services becomes more critical

In many countries and financial i

And international bankings and sec

To ensure viability of

When pharm

They are

Question 6

Consider the statement ‘‘Business continuity planning is only about recovery of computer systems.” Is it true or false? Explain your reasoning.

False

Past, recovery of computer and tech systems.This discipline is oft as

Recovery of IT functions alone does not ensure the survival of an

In the past, continuity planning was frequently thought of as the recovery of computer or information technology systems and nothing more. This discipline is often referred to as disaster recovery planning. Experience in the field of continuity planning has shown that the recovery of IT functions alone does not ensure survival of the enterprise following a serious disruption or disaster. Complete recovery requires thorough knowledge of all aspects of the enterprise.

Question 7

Does business continuity planning provide any additional benefits to an organisation apart from providing the ability to recover from major disruptive events.

THere are other less benefits of other

The business continuity planner must understand the processes of his enterprise and how his services goods moves within the

Cash flow in and out of the enterprise. The collection and analysis of this knowledge ca

Creating efficiencies,

Planner may also find opp in cost savings in insurance and

Eg. shows that BCP can provide an advantage over competitors

COntinuity process

Vital records management, data backup storage and

And efficiencies may be discovered during bcp process

There are other, less obvious benefits of continuity planning. In developing a comprehensive continuity planning infrastructure, the continuity planner must understand the business processes of his enterprise, and how information, goods, and services move within the organization. Equally important is knowing how information, goods, services, and cash flow in and out of the enterprise.

The collection and analysis of this knowledge could identify potential cost reductions by improving or creating operating efficiencies. The planner may also find opportunities for cost savings in business interruption insurance and directors and officer's coverage. These examples show that continuity planning could provide an advantage over competitors. As the importance of continuity planning becomes more well known, the lack of planning could even disqualify a company from consideration for new business.

The continuity planning process also forces a review of various other components of the organization's infrastructure. Vital records management, data backup and storage, and physical, environmental, and information security controls must also be scrutinized when addressing continuity planning, and efficiencies may be discovered during the process

Question 8

Describe the advantages and disadvantages of hot sites

Available as soon as possible

Usually used for short termed services but available for long term stay

Disadv: expensive and limited on hardware and software choices

Hot Sites' Advantages

* Ready within hours for operation
* Highly available
* Usually used for short-term solutions, but available for longer stays
* Annual testing available

Hot Sites’ Disadvantages

* Very expensive
* Limited on hardware and software choices

Question 9

Describe the advantages and disadvantages of cold and warm sites.

ADv: Less expensive

Available for longer timeframe bec of reduced costs

Practical for proprietary software

Disa: Op testing not avail

Res for not readily available

Warm and Cold Sites' Advantages

• Less expensive

• Available for longer time frames because of the reduced costs

• Practical for proprietary hardware or software use

Warm and Cold Sites' Disadvantages

• Operational testing not usually available

• Resources for operations not immediately available

Question 10

What is the fundamental difference between recovery time objective (RTO) and maximum tolerable downtime (MTD)? Suppose that RTO has been fixed, which aspects of data backup could be influenced by MTD? Discuss.

Diff:

RTO is the specified time or recovering critical or core functions

Eg. website is up but w only limited or core features

In contrast, MTD it is the max time frame

Discuss: second stage governed by WRT

When rto is fixed, the

If MTD is large, the recovery time is large, any recovery stage

If MTD is small, the recovery time is small, differential

If MTD is very small, we need high,

Data mirroring and full backup is needed

Difference: RTO is the specified time frame for recovering critical infrastructure/core functions of an organization, for example the website is up but with only limited/core features. In contrast, MTD is the specified time frame for bringing back the whole system to normal, which means all features should be available just like before the disaster strikes.

• Discussion: The data recovery is actually done in the second stage and is governed by WRT, which is MTD-RTO. When RTO is fixed, the time for recovering data is directly dependent on MTD:

- If MTD is large, the data recovery time is large, hence any backup method, such as incremental backup is ok as we can take several steps to actually recover the data

- If MTD is small, the data recovery time is small, we need to recover data quickly, so differential backup might be preferred as it takes less time

- If MTD is very small, just sufficient for other testing, we need high availability, which mean data mirroring/redundancy/full backup is required.

Question 11

What are the the MTD, RPO, RTO values of the following scenario: Susan is the new BCM coordinator and needs to identify various preventive and recovery solutions her company should implement for BCP/DRP efforts. She and her team have carried out an impact analysis and found out that the companys order processing functionality cannot be out of operation for more than 15 hours. She has calculated that the order processing systems and applications must be brought back online within eight hours after a disruption. The analysis efforts have also indicated that the data that are restored cannot be older than five minutes of current real-time data.

MTD: 15 hours

RTO: 8hrs

RPO: 5 minutes

The

The systems and operations have to be running

Work recovery time 7hrs

WRT deals w restoring data, testing processes and making everything live.

Thus

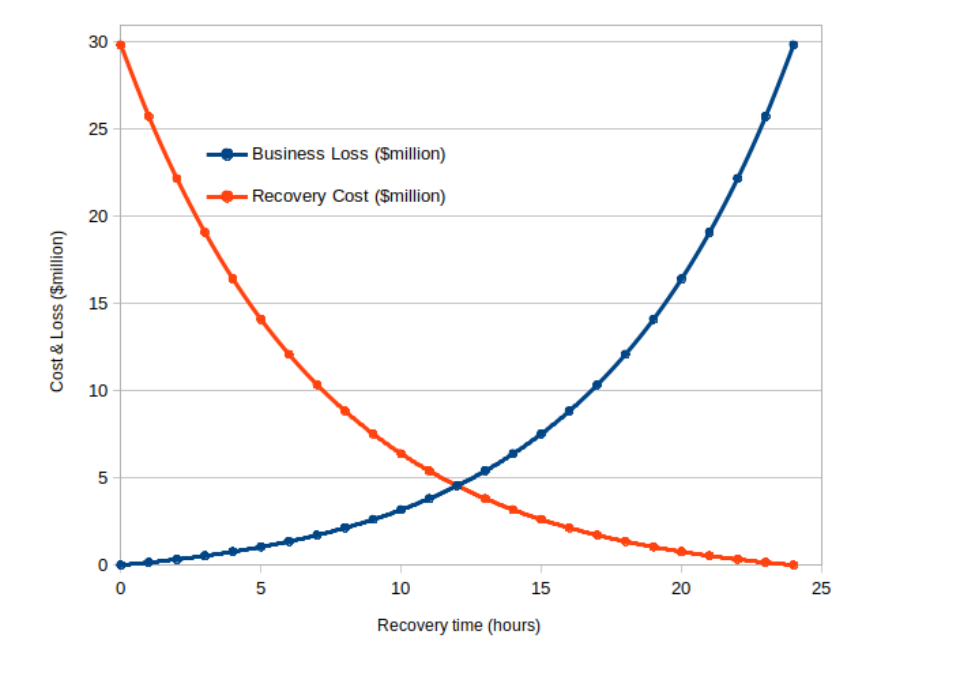
MTD of the order processing functionality is 15 hours. RTO value is 8 hours. WRT value is 7 hours.

RPO value is 5 minutes.

The order processing functionality as a whole has to be up and running within 15 hours. which is the maximum tolerable downtime (MTD). The systems and applications have to be up and running in eight hours, which is the Recovery Time Objective (RTO. RTO deals with technology, but we still need processes and people in place to run the technology. Work Recovery Time (WRT) is the remainder of the overall MTD value. RTO usually deals with getting the infrastructure and systems back up and running, and WRT deals with restoring data, testing processes, and then making everything live for production purposes. The data that are restored for this function can only be five minutes old; thus, the Recovery Point Objective (RPO) has the value of five minutes.

Question 12

The BIA team of an organisation is determining the recovery time of their core system due to a disaster. The team has been able to plot the relationships between the business loss (due to ceasing of critical business activities) and the recovery cost (due to offsite facility and other related expenses) against recovery time below. The core system definitely needs to be recovered within 24 hours and the BIA team believes that a much quicker recovery can be achieved. Suppose that this is the only information available, suggest the optimal recovery time that the BIA team should aim for and explain your suggestion. Your argument must be based on the plot given below.



\*Find optimum point which is intersection betw 2 curves = 12hrs

If recovery time is less than 12 hrs, the recovery cost is more than the loss - not worth it

While longer recover

Sum of the two curves

Total cost of 9.1mil. Much less than 31 mil perceived as maximum absorbed cost

In the absence of other information, intersection is the

Students are expected to find the optimal point being the intersection between two curves, which is exactly 12 hours (the two curves have been specially created). They are also expected to explain that if recovery time is less than 12 hours the recovery cost is much more than the loss and it is not worth spending that much, whilst longer recovery time can significantly increase business loss.

Furthermore, if the total cost is taken into account, the sum of the two curves also gives the minimum at that intersection (which gives a total cost of $9.1 millions, still much less than $30 millions perceived as maximum absorbed cost). In the absence of other information, the intersection is the best choice as far as the cost and loss are concerned

Question 13 What are the three main phases in a contingency plan as per the NIST SP800 standard? Briefly describe the activity in each phase.

1. Activation and notification phase is. Phase includes activities that
2. REcovery: Activities

Students are expected to look up the NIST SP800 standard before answering this question.

* Phase 1 - Activation and notification: The Activation and Notification Phase defines initial actions taken once a system disruption or outage has been detected or appears to be imminent. This phase includes activities to notify recovery personnel, conduct an outage assessment, and activate the plan. At the completion of the Activation and Notification Phase, information system contingency plan (ISCP) staff will be prepared to perform recovery measures to restore system functions.
* Phase 2 - Recovery: Recovery Phase activities focus on implementing recovery strategies to restore system capabilities, repair damage, and resume operational capabilities at the original or new alternate location. At the completion of the Recovery Phase, the information system will be functional and capable of performing the functions identified in the plan. Depending on the recovery strategies defined in the plan, these functions could include temporary manual processing, recovery and operation at an alternate system, or relocation and recovery at an alternate site. It is feasible that only system resources identified as high priority in the BlA will be recovered at this stage.
* Phase 3 - Reconstitution: The Reconstitution Phase is the third and final phase of ISCP implementation and defines the actions taken to test and validate system capability and functionality. During Reconstitution, recovery activities are completed and normal system operations are resumed. If the original facility is unrecoverable, the activities in this phase can also be applied to preparing a new permanent location to support system processing requirements. This phase consists of two major activities: validating successful recovery and deactivation of the plan.