Question 1

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

解释业务连续性计划（BCP）和灾难恢复计划（DRP）的根本区别。

Students 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

学生应该参考BCP的讲座幻灯片，认识到DRP是BCP的一个子组成部分（BCP包括：BIA、COOP+DRP、测试和维护）。BCP是一个过程，旨在减少组织生存所需的关键功能/操作（手动或自动）的意外中断所带来的业务风险，而DRP通常详细说明IT个人在灾难发生后恢复计算机系统和操作设施的过程。

Question 2

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

什么是业务影响分析（BIA），它的用途是什么？

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:

BIA是BCP的第一个阶段。作为初始规划阶段的一个重要组成部分，它是对各种事件可能对组织产生的影响的调查和评估。它包括:

* Determine core business processes and recover criticality

确定核心业务流程和恢复的关键性

* Identify resource requirements

确定资源需求

* Identify recover priorities for system resources

确定系统资源的恢复优先级

Question 3

What is the fundamental difference between BIA and risk assessment?

BIA和风险评估之间的根本区别是什么？

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.

风险管理的重点是识别威胁、漏洞和攻击，以确定能够保护数据的控制措施。另一方面，BIA假设这些控制措施已经失败/未通过/无效，并且攻击已经成功。因此，BIA处理最坏的情况。

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.

紧急情况或灾害管理的综合方法通常包括四个阶段。预防、准备、响应和恢复（PPRR）。业务影响分析（BIA）属于哪个阶段？描述两（2）个典型软件公司的关键活动的例子，这些活动需要作为业务影响分析的一部分来建立。

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

BIA属于: 准备工作

一家软件公司与QLD BCP指南中的制造公司类似，因此可以找到类似的例子如下

确保与客户签订合同

开发软件

交付和支持开发的软件产品

Question 5

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

解释为什么大型组织拥有适当的BCP很重要？如果发现缺乏BCP，会有什么影响？

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.

法律和法规要求：许多行业可能发现自己受到联邦、州和地方法律或法规的约束，要求他们实施不同程度的业务连续性规划。例如，上市公司的高管和董事有信托责任，在执行业务连续性职责时要尽职尽责。在其他情况下，要求（和失败的后果）可能更严重。紧急服务，如警察、消防和紧急医疗行动，对社区有责任在发生灾难时继续运作。事实上，当公共安全受到威胁时，他们的服务在紧急情况下变得更加重要。如果他们不能实施一个可靠的BCP，可能会导致生命和/或财产的损失，以及民众对政府的信心下降。

In many countries, financial institutions, such as banks, brokerages,and the firms that process their data, are governed by strict government and international banking and 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.

在许多国家，金融机构，如银行、经纪公司和处理其数据的公司，都受到严格的政府和国际银行和证券法规的约束，旨在促进其继续运作，以确保国民经济的生存能力。为什么药品制造商必须在灾难后不太理想的情况下生产产品，他们被要求向政府监管机构证明其产品的纯度。还有无数其他的例子，这些行业被各种法律和法规要求在紧急情况下继续运营。

Question 6

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

考虑一下''业务连续性计划只是关于计算机系统的恢复 "的说法。它是真的还是假的？解释一下你的推理。

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.

在过去，连续性规划经常被认为是计算机或信息技术系统的恢复，仅此而已。这门学科通常被称为灾难恢复规划。连续性规划领域的经验表明，仅仅恢复信息技术功能并不能确保企业在发生严重中断或灾难后的生存。完整的恢复需要对企业的所有方面有全面的了解。

Question 7

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

除了提供从重大破坏性事件中恢复的能力外，业务连续性规划是否为一个组织提供任何额外的好处。

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.

连续性规划还有其他一些不太明显的好处。在开发全面的连续性规划基础设施时，连续性规划人员必须了解企业的业务流程，以及信息、货物和服务如何在组织内流动。同样重要的是了解信息、货物、服务和现金如何在企业内流动和流出。

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.

对这些知识的收集和分析可以通过改善或创造运营效率来确定潜在的成本削减。规划者还可能发现在业务中断保险和董事及高级职员保险方面节省成本的机会。这些例子表明，连续性规划可以提供相对于竞争对手的优势。随着连续性规划的重要性越来越广为人知，缺乏规划的公司甚至会被取消新业务的考虑资格。

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

连续性规划过程也迫使人们对组织的基础设施的各种其他组成部分进行审查。重要的记录管理、数据备份和存储，以及物理、环境和信息安全控制，在处理连续性规划时也必须进行仔细审查，在这个过程中可能会发现效率。

Question 8

Describe the advantages and disadvantages of hot sites

描述热点网站的优势和劣势

Hot Sites' Advantages热门网站的优势

* Ready within hours for operation 几小时内即可投入使用
* Highly available 高度可用
* Usually used for short-term solutions, but available for longer stays

通常用于短期解决方案，但可用于较长时间的停留

* Annual testing available 可进行年度测试

Hot Sites’ Disadvantages 热门网站的劣势

* Very expensive 非常昂贵
* Limited on hardware and software choices 在硬件和软件选择上受到限制

Question 9

Describe the advantages and disadvantages of cold and warm sites.

描述的 cold and warm sites 的优势和劣势。

Warm and Cold Sites' Advantages 优势

* Less expensive 价格较低
* Available for longer time frames because of the reduced costs

由于成本降低，可用于更长的时间框架

* Practical for proprietary hardware or software use

适用于专有硬件或软件的使用

Warm and Cold Sites' Disadvantages

* Operational testing not usually available

通常不提供操作测试

* Resources for operations not immediately available

无法立即获得的行动资源

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.

恢复时间目标（RTO）和最大可容忍停机时间（MTD）的根本区别是什么？假设RTO已经固定，那么数据备份的哪些方面可能会受到MTD的影响？讨论一下。

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.

区别。RTO是指恢复组织的关键基础设施/核心功能的特定时间框架，例如，网站已经启动，但只有有限的/核心的功能。相比之下，MTD是将整个系统恢复到正常状态的规定时间，这意味着所有的功能都应该像灾难发生前那样可用。

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:

讨论。数据恢复实际上是在第二阶段进行的，并受WRT的制约，也就是MTD-RTO。当RTO是固定的，恢复数据的时间就直接取决于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

如果MTD很大，数据恢复时间也很大，因此任何备份方法，如增量备份都可以，因为我们可以采取几个步骤来实际恢复数据。

* 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

如果MTD较小，数据恢复时间较短，我们需要快速恢复数据，所以差分备份可能是首选，因为它花费的时间较短。

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

如果MTD非常小，只够用于其他测试，我们需要高可用性，这意味着需要数据镜像/冗余/完整备份。

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.

以下情景的MTD、RPO、RTO值是多少。苏珊是新的BCM协调员，需要确定她的公司应该为BCP/DRP工作实施的各种预防和恢复解决方案。她和她的团队进行了一次影响分析，发现公司的订单处理功能不能停止运行超过15小时。她计算了一下，订单处理系统和应用程序必须在中断后8小时内恢复在线。分析工作还表明，恢复的数据不能超过当前实时数据的5分钟。

MTD of the order processing functionality is 15 hours. RTO value is 8 hours. WRT value is 7 hours. RPO value is 5 minutes.

订单处理功能的MTD是15小时。RTO值为8小时。WRT值是7小时。RPO值为5分钟。

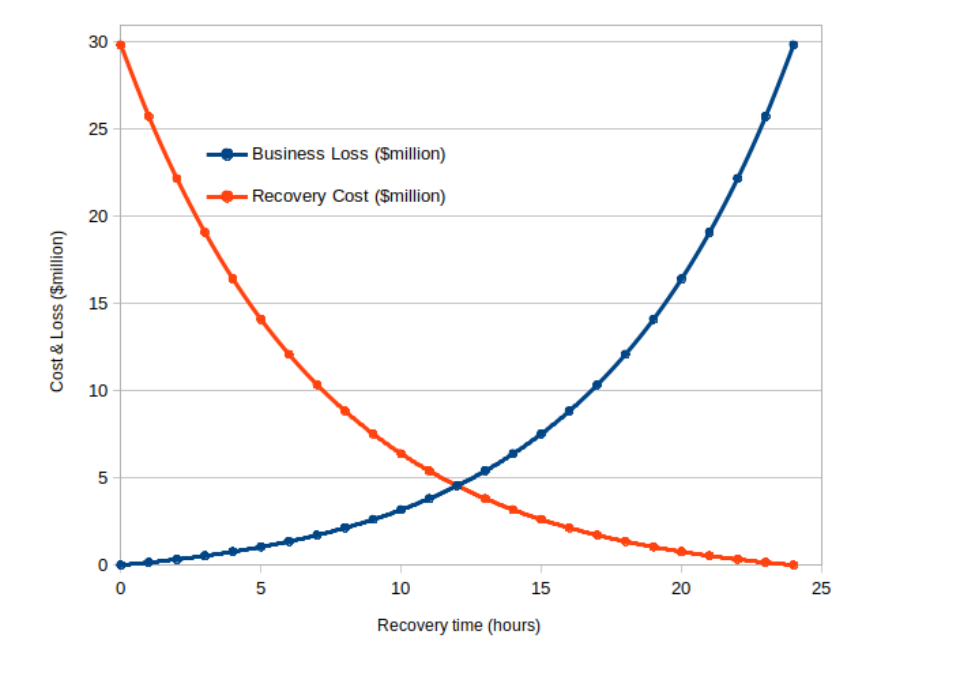
The order processing functionality as a whole has to be up and running within 15 hours. which is the maximum tolerable downtime (MTD). The systems and applications have to be up and running in eight hours, which is the Recovery Time Objective (RTO. RTO deals with technology, but we still need processes 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.

订单处理功能作为一个整体必须在15小时内启动和运行，这是最大可容忍的停机时间（MTD）。系统和应用必须在8小时内启动并运行，这是恢复时间目标（RTO）。RTO处理的是技术，但我们仍然需要流程和人员到位来运行技术。工作恢复时间（WRT）是整个MTD值的剩余部分。RTO通常处理的是让基础设施和系统恢复运行，WRT处理的是恢复数据，测试流程，然后让一切都为生产目的而运行。为这个功能恢复的数据只能是5分钟前的，因此，恢复点目标（RPO）的值是5分钟。

Question 12

The BIA team of an organization 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.

一个组织的BIA团队正在确定他们的核心系统在灾难中的恢复时间。该团队已经能够绘制出业务损失（由于关键业务活动的停止）和恢复成本（由于异地设施和其他相关费用）与恢复时间之间的关系。核心系统肯定需要在24小时内恢复，BIA团队认为可以实现更快的恢复。假设这是唯一可用的信息，建议BIA团队应该争取的最佳恢复时间并解释你的建议。你的论点必须基于下面给出的情节。



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

\*找到2条曲线的交点的最佳点=12小时

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.

学生们要找到最佳点，即两条曲线的交点，正好是12小时（这两条曲线是专门创建的）。他们还需要解释，如果恢复时间少于12小时，恢复成本就会远远超过损失，不值得花这么多钱，而更长的恢复时间会大大增加企业损失。

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

此外，如果考虑到总成本，两条曲线的总和也给出了该交叉点的最小值（这给出了910万美元的总成本，仍然远远低于被认为是最大吸收成本的3000万美元）。在没有其他信息的情况下，就成本和损失而言，该交叉点是最佳选择。

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.

根据NIST SP800标准，应急计划的三个主要阶段是什么？简要描述每个阶段的活动。

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

在回答这个问题之前，学生应该先查一下NIST SP800标准。

* 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.

阶段1--启动和通知。激活和通知阶段定义了一旦发现或似乎即将发生系统破坏或中断时采取的初步行动。这个阶段包括通知恢复人员、进行故障评估和启动计划的活动。在启动和通知阶段完成后，信息系统应急计划（ISCP）人员将准备好执行恢复措施，以恢复系统功能。

* 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.

第二阶段 - 恢复。恢复阶段的活动重点是实施恢复战略，以恢复系统能力，修复损坏，并在原地或新的替代地点恢复运行能力。在恢复阶段完成后，信息系统将具备功能，能够执行计划中确定的功能。根据计划中确定的恢复策略，这些功能可能包括临时的手工处理，在备用系统中的恢复和操作，或者在备用地点的搬迁和恢复。在这个阶段，只有在BlA中被确定为高优先级的系统资源才会被恢复，这是可行的。

* 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.

第三阶段--重构。重建阶段是ISCP实施的第三个也是最后一个阶段，它定义了为测试和验证系统能力和功能而采取的行动。在重建过程中，恢复活动已经完成，正常的系统操作已经恢复。如果原来的设施无法恢复，这个阶段的活动也可以应用于准备一个新的永久地点来支持系统处理的要求。这个阶段包括两个主要活动：验证成功恢复和停用计划。