



ITIL® Intermediate Capability Stream:

PLANNING, PROTECTION AND OPTIMIZATION (PPO) CERTIFICATE

Sample Paper 2, version 6.1

Gradient Style, Complex Multiple Choice

QUESTION BOOKLET

**Gradient Style Multiple Choice
90 minute paper
8 questions, Closed Book**

Instructions

- 1. All 8 questions should be attempted.*
- 2. You should refer to the accompanying Scenario Booklet to answer each question.*
- 3. All answers are to be marked on the answer grid provided.*
- 4. You have 90 minutes to complete this paper.*
- 5. You must achieve 28 or more out of a possible 40 marks (70%) to pass this examination.*

Question One

Refer to Scenario One

You have recently joined the information security management team within the IT organization and have been asked by the chief information officer (CIO) to produce an information security policy for the TC company.

Which one of the following options provides the MOST CORRECT summary of the contents of the information security policy, and MOST CORRECTLY identifies who should authorize the policy?

- A. The information security policy should cover all areas of security and should be appropriate for the needs of the business. It should include the management procedures that support the policy and should contain the policy for providing access to IT services and information to TC's suppliers. The information security policy should also contain an asset control policy for the call centres and retail outlets, and should mandate how assets must be disposed of when they are de-installed. The policy should be authorized by the chief executive officer (CEO) of TC on behalf of the business and the IT organization.
- B. The information security policy should include the existing email and internet usage policies. It should include the policies relating to passwords and access to TC's IT systems. The information security policy should contain an information classification policy and a document classification policy. The information security policy should state how it will be maintained, with reviews on an, at least, annual basis. The information security policy should be authorized by the CEO on behalf of both IT and the business. The information security policy should contain a distribution list so that it can be communicated to all of the IT organization's customers and users, as well as to IT staff in the call centres.
- C. The information security policy should be authorized by the information security manager. It should include the management procedures that relate to information security and should document the security controls that will be implemented. The information security policy should specify what tools will be used to prevent security incidents and what tools and processes will be used to detect security incidents. The information security policy should also define the process for emergency changes and identify who in TC can authorize them.
- D. The information security policy should contain a statement from the CIO advising that compliance with the policy is mandatory for all staff within TC. The policy should contain the process for all staff to undergo information security awareness training and should also contain the responsibilities for implementing the policy within the IT organization. The email usage and internet usage policies should be included within the information security policy. The information security policy should be issued to all new call centre staff as part of the induction process. The information security policy should be authorized by the CIO on behalf of the IT organization.

Question Two

Refer to Scenario Two

The service manager has asked you to evaluate the three proposals. Which one of the following options is the BEST approach?

- A. The insurance company should migrate all of its service management tool use to company C's tool set. This will allow the insurance company to have the advantage of a fully integrated suite of tools from the market leader.
- B. The insurance company should upgrade to the new version of company B's product (including non-IT data) and purchase the extractor for company A's data when it becomes available. This will address the issue of data incompatibility whilst allowing all users to continue to use the tools with which they are familiar.
- C. The insurance company should migrate all of its service management tools to company C's tool set because it includes all necessary current design tools functionality. To leverage the migration time wisely, the designers should switch from company B's tools to company C's tools during the migration in order to gain familiarity with the tools.
- D. The insurance company should migrate its design tools to company A's product when it becomes available. This will have the advantage of an integrated tool set using transition and operations tools with which users are already familiar.

Question Three

Refer to Scenario Three

You are a member of staff within the managed service provider company and have been given responsibility for designing the capacity management and IT service continuity management processes for the IT organization. Your initial task is to identify the most serious risks facing the service provider.

Which one of the following options is the BEST summary of the MOST SERIOUS risks that the service provider will face?

- A.
 - The IT service continuity management plan held by the IT organization's teams might not be adequately version-controlled, as the plan will be issued by the service provider.
 - The service provider will need to rely on tools and technology to provide the warnings and alerts to enable effective capacity management.
 - The lack of technical involvement by the IT organization in the design phase may mean that the IT organization's requirements are not fully considered.
- B.
 - The government department will assume that all activities relating to its business continuity will be managed by the service provider without the involvement of the IT organization.
 - The business continuity plan and IT service continuity plan will not be sufficiently aligned.
 - The results of the information security management risk assessment may not be provided to the service provider, resulting in poor alignment of the risk management process between the two organizations.
- C.
 - The service provider does not have visibility of the overall business continuity management plan and process.
 - Availability management and information security management remain the responsibility of the IT organization, and the information used by these two processes may not be shared with the capacity management and IT service continuity management processes.
 - A lack of technical involvement by the IT organization in the design phase may mean that the IT organization's requirements are not fully considered.
- D.
 - There may be a lack of management commitment within the service provider to provide the necessary resources and budget to design the services appropriately.
 - Combining the roles of IT service continuity manager and capacity manager will not be effective because these roles are incompatible.
 - The IT service continuity and capacity manager's involvement in the CAB will be a distraction and will reduce time spent on primary responsibilities.

Question Four

Refer to Scenario Four

You are the design co-ordination manager. You see this new service as a way to demonstrate the value of integration among service design processes. The managers of the design processes, however, are reluctant to change the way they work. You ask them to attend a meeting at which you will present what you believe are the most compelling arguments for co-ordination.

Which of the following options is the MOST CORRECT set of design process integration points for THIS new service?

- A. The areas where integration is most critical are:
- Working with change management to determine planned service outages (PSOs)
 - Preparation of the availability testing plan
 - Determination of Vital Business Functions (VBFs)
 - Establishment of recovery options
- B. The areas where integration is most critical are:
- Undertaking risk assessment activities
 - Establishment of recovery options
 - Determination of Vital Business Functions (VBFs)
 - Working with change management to determine planned service outages (PSOs)
- C. The areas where integration is most critical are:
- Determining the amount of resilience needed to provide the required availability
 - Establishment of recovery options
 - Determination of Vital Business Functions (VBFs)
 - Undertaking risk assessment activities
- D. The areas where integration is most critical are:
- Preparation of the availability testing plan
 - Working with change management to determine planned service outages (PSOs)
 - Development of the preventive maintenance schedule
 - Working with problem management to update the known error data base (KEDB)

Question Five

Refer to Scenario Five

You have been appointed as the manager for IT service continuity management (ITSCM) and you have been asked to make recommendations for implementing ITSCM.

Which one of the following options is the BEST set of recommendations for developing an ITSCM strategy and for implementing effective ITSCM?

- A. A lifecycle approach should be adopted for implementing ITSCM. The first stage is initiation, followed by requirements and strategy, implementation, and ongoing operation. In the initiation stage the ITSCM manager will work with business operations to define the scope of ITSCM. The ITSCM manager will plan the business impact analysis (BIA) and risk assessment (RA) activities that will be undertaken by the ITSCM team. The output from the BIA and RA will be used to determine the business continuity strategy and the underpinning ITSCM strategy.
- B. A lifecycle approach should be adopted for implementing ITSCM. The four stages are strategy, design, transition, and operation. The best way of implementing effective ITSCM is through the identification of critical technology components and ensuring that these are continuously available. Therefore ITSCM will be used to ensure that the IT infrastructure and environment will always be available regardless of external factors. Once appropriate technology has been identified, business operations will be informed of the costs and other implications of this solution.
- C. A lifecycle approach should be adopted for implementing ITSCM. The four stages are strategy, design, transition, and operation. The first two stages involve business impact analysis (BIA) and risk assessment (RA). Business operations will be involved in these two stages in order to support the ITSCM activities and to understand the relationship between business processes and the IT services that support them. As a result of these initial BIA and RA activities, an ITSCM strategy should be produced and used to drive the business continuity strategy.
- D. A lifecycle approach should be adopted for implementing ITSCM. The first stage is initiation, followed by requirements and strategy, implementation, and ongoing operation. The IT organization and business operations will work together to understand the relationship between business processes and the IT services that support them. Once business impact analysis (BIA) and risk analysis (RA) activities are complete, business operations will be responsible for producing a business continuity strategy. Following this, an ITSCM strategy should be produced that underpins the business continuity strategy and its needs.

Question Six

Refer to Scenario Six

You are a member of the IT organization and have been asked to develop an action plan to address the issues with the reporting service.

Which one of the following options is the MOST appropriate set of actions to take?

- A.
 - Start collecting data regarding report generation, viewing activity, and corresponding component utilization
 - Identify normal patterns of activity and use these to set thresholds and create incidents when a service level has been breached
 - Improve performance by identifying resource-intensive activities and running them overnight
 - Reschedule the security software so that it does not run between the hours of 9:00 a.m. and 5:00 p.m.
 - Understand the nature of future report generation and viewing requests as staffing levels increase.
- B.
 - Implement monitoring of servers and set thresholds according to well-known technology limits, e.g. 70% central processing unit (CPU) utilization
 - Generate automatic incidents when the thresholds are exceeded
 - Implement response time monitoring by generating test report requests at peak times and measuring their performance
 - Set the security software to run at midnight when the servers are less busy
 - Collect statistics on resource utilization and predict future demand using statistical trending techniques based on historic analysis.
- C.
 - Record all report generation and viewing activity and measure the utilization and performance of the underlying technology
 - Analyse current trends and use this data to understand the impact of future workloads
 - Set thresholds to warn of possible degradations of service
 - Identify resource-intensive report requests and investigate whether these can be scheduled at less disruptive times
 - Determine whether the security software causes degraded response times and consult with the IT security manager to learn about possible alternatives.
- D.
 - Identify peak periods and use modelling techniques to determine appropriate technology upgrades
 - Evaluate the anticipated growth in report demand and include this in the upgrade plans
 - Encourage users to submit their report viewing requests overnight
 - Prohibit the running of requests to generate or view reports between 10:00 a.m. and 1:00 p.m. when the security software is running
 - Monitor the number of reports being requested and use software to limit the number of requests that can be processed simultaneously.

Question Seven

Refer to Scenario Seven

To help with the repackaging effort, you have been asked to develop a service package of core services and service options for the services provided by the organization.

Which one of the following options is the MOST appropriate combination of core services and associated service options to meet the needs of the organization's customers?

- A. The core services would allow customers to access the service desk and would provide guaranteed confidentiality. The core services would also provide access to a limited number of standard reports (activity 4). Access to all standard reports would be available as a service option. Activities 1, 2 and 3 would be available as separate service options, and would also be bundled into a single service option. Activity 5 would be available as another service option.
- B. The core services would allow customers to access the standard reports through a login username and password (activity 4). Activities 3 and 5 would be included in the core services. Each of the five activities would be made available as separate service options, allowing customers to select the specific combination of service options they require. Access to the service desk and a guarantee of confidentiality would be bundled together and made available as another service option.
- C. The core services would allow customers to access the service desk. Access to any of the standard reports would also be included in the core services (activity 4). Activities 1, 2 and 3 would be available as separate service options. Activities 1, 2 and 3 would also be bundled together as a single service option. Activity 5 would be available as another service option. Guaranteed confidentiality would also be available as a service option.
- D. The core services would allow customers to access any of the standard reports (activity 4). Access to the service desk and a guarantee of confidentiality would be bundled together into a single service option. Activities 1 and 2 would be bundled together into another service option. Activities 1 and 2 would also be available as separate service options to give customers greater choice. Activities 3 and 5 would be available as separate service options.

Question Eight

Refer to Scenario Eight

You have been asked by the chief information officer (CIO) to identify a small number of key performance indicators (KPIs) that should be reviewed regularly. Your first task is to identify KPIs most relevant to the recent problems experienced by the business.

Which one of the following options is the MOST appropriate set of KPIs that are relevant to the recent problems experienced by the business?

- A.
 - Percentage reduction in the number of events recorded
 - Improvement in the accuracy of forecasts of business trends and workload
 - Percentage reduction in the unavailability of services and components
 - Reduction in the mean time to restore service (MTRS).
- B.
 - Percentage improvement in the overall availability of IT services
 - Percentage reduction in the number of failures during critical business periods
 - Percentage reduction in the amount of staff overtime due to the unavailability of IT services
 - Improvement in the mean time between failures (MTBF).
- C.
 - Number of updates to the projected service outage (PSO) document
 - Improvement in the accuracy of recording incidents related to unavailability
 - Reduction in mean time between service incidents (MTBSI)
 - Percentage increase in the time spent on the management of the availability management plan.
- D.
 - Improved perception of the service management processes by the business
 - Number of incidents which impact on the availability of IT services to users
 - Percentage reduction in the number of incidents that have been incorrectly assigned thereby causing unavailability
 - Percentage increase in the reliability of IT service components.