ITIL® Intermediate Lifecycle Stream:

SERVICE OPERATION CERTIFICATE

Sample Paper 1, 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

Which one of the following options BEST summarizes the risks that the IT organization currently does and does not face?

A.
- Resistance to change within IT is a risk
- Differing customer and IT expectations are a risk
- Lack of testing is NOT a risk
- Lack of involvement of IT operations staff in other lifecycle activities is NOT a risk

B.
- Reliance on key personnel along with their knowledge and skill is a risk
- Lack of adequate tools is a risk
- Lack of business support is NOT a risk
- Inadequate funding is NOT a risk

C.
- Reliance on key personnel along with their knowledge and skill is a risk
- Lack of business support is a risk
- Resistance to change within IT is NOT a risk
- Inadequate funding is NOT a risk

D.
- Resistance to change within IT is a risk
- Inadequate funding is a risk
- Alignment of IT with the business is NOT a risk
- Lack of involvement of IT operations staff in other lifecycle activities is NOT a risk

Question Two

Refer to Scenario Two

You have been asked to review the application management, application development and IT operations management functions and identify the causes of the issues.

Which one of the following set of options is MOST LIKELY to be causing the issues experienced by this organization?

A.
- Application management has failed to obtain information about known errors from software suppliers
- IT operations management has failed to define and provide application training to users
- Application management has failed to involve IT operations staff in application deployment activities

B.
- Application management has not developed and implemented a set of standards for application architecture
- Application management is not providing the resources required for third-line support for the resolution of incidents and problems
- Application management has not adequately defined operational models or defined the technical resources required to operate the applications in the live environment

C.
- Application management has not developed and implemented a set of standards for application architecture
- Application management and application development have failed to provide information about known errors to IT operations management teams
- Application development has failed to provide the resources required for third-line support for the resolution of incidents and problems

D.
- Application management has not participated in testing the functionality of applications
- Application management has failed to identify and fulfil training needs required to manage and operate applications
- Application management has not adequately defined operational models or defined the technical resources required to operate the applications in the live environment

Question Three

Refer to Scenario Three

You are the team leader responsible for monitoring and control. You are required to resolve the issues arising in the scenario and reach a conclusion.

Which one of the following options is the BEST solution to address the data retention issues?

A.
- You consult the problem, capacity, availability and security management teams to gain a more detailed understanding of their event data requirements
- You take into account the suggestions of the organization's legal department regarding the legislative and compliance issues
- You define and document a policy that ensures that all informational event data is retained for a minimum of six years and three months

B.
- The legal requirement is the most important as non-compliance could incur fines for the company, so you consult the legal and compliance departments to further categorize the data and agree how long each should be retained
- You consult the problem, capacity, availability and security management teams and confirm the need for the one year retention and six month retention periods and identify any further data categories relevant to these teams
- You create a retention policy to document these requirements

C.
- You agree that this data is extremely unlikely to be needed beyond one week and that, on the balance of risk, the cost of retaining this data outweighs the need
- In order to achieve the most cost-effective solution, you document and implement the one-week retention policy
- You advise the legal department of your decision in case any related IT governance issues arise in the future

D.
- You consult the business users and the IT groups that might use the data, and hold specific discussions with the legal and compliance departments to identify their requirements
- You create clear criteria to identify each event-type and you define a retention period for each in accordance with the specific business need
- You create a retention policy to document these requirements

Question Four

Refer to Scenario Four

You have been asked to advise whether any process-related changes should be made to the way the company handles these service requests in the future.

Which one of the following recommendation options BEST reflects ITIL guidance?

A.
- As a large proportion of service desk calls are service requests, a separate request fulfilment process should be recommended to channel these to the appropriate groups quickly without impact on critical or high-priority incidents
- Providing access for temporary staff/contractors is not a type of service request and a separate access management process should be set up to handle these
- A business case must be made to justify the costs involved in setting up and running the new processes

B.
- An organization needs only to implement a separate request fulfilment process where this is fully justified. As the service desk is well regarded in this case, it appears that no immediate action is needed
- As there is no clear proof, only anecdotal evidence, that handling service requests through the current incident management process is causing any difficulties, no action is required
- The situation should be monitored and the figures analysed and reviewed again in three months' time to see whether any process change is necessary

C.
- As a large proportion of service desk calls are service requests, a separate request fulfilment process should be recommended to channel these to the appropriate groups quickly and without impact on critical or high priority incidents
- A web-based self-help capability should be considered as this may help make some level of support available outside normal office hours
- A business case must be made to justify the costs involved in setting up and running the new process

D.
- New user set-ups and workstation moves are changes and requests for change (RFCs) should be raised, so these calls should not be handled as service requests
- As these types of requests represent a large percentage of calls to the service desk a further review is required before a decision is made to implement a separate request fulfilment process
- A web-based self-help capability should be considered as this may help make some level of support available outside normal office hours

Question Five

Refer to Scenario Five

Which one of the following options BEST summarizes the remaining steps in the process that you will communicate to the service desk and second-line support staff?

A.
- Ensure service desk staff can establish the impact and urgency of incidents so that the key services are dealt with in business need order
- If no resolution can be identified by the service desk and the incident is a recurring desktop issue then a problem record will be raised and allocated to the appropriate technical teams in order to avoid unnecessary call out charges from the supplier
- Once the problem is resolved, a known error record will be created and, if necessary, a request for change (RFC) will be raised

B.
- Base incident priority on impact and urgency, where impact codes have been agreed in advance by service level management to ensure that the key services are dealt with in business need order
- If the incident is related to the holiday booking service then it is escalated immediately before the service desk identify a resolution, to be investigated by the appropriate technical teams
- If a resolution cannot be identified or it is considered necessary to identify the cause of the incident, a problem record will be raised

C.
- Base incident priority on impact and urgency, where impact codes have been agreed in advance by service level management to ensure that the key services are dealt with in business need order
- If no resolution can be identified by the service desk then the incident is escalated to the appropriate technical teams who will investigate the incident and seek a resolution
- If a resolution cannot be identified or it is considered necessary to identify the cause of the incident, a problem record will be raised

D.
- Base incident priority on the urgency of the issue to ensure that the key services are dealt with in business need order
- If no resolution can be identified by the service desk then a problem record will be raised and allocated to the appropriate technical teams who will seek the cause and a workaround
- Once the problem is resolved, a known error record will be created and, if necessary, an RFC will be raised

Question Six

Refer to Scenario Six

Which one of the following approaches will BEST enable you to assess each function's capabilities and level of maturity?

A.
- Conduct a skills inventory and determine if the staff's technical certifications are up to date
- Review training plans and survey the technical staff to determine if they are getting the technical training they feel they need
- Review and assess the quality of technical documentation, including the escalation procedures that are executed in incident management
- Review incident response times, the number of escalations and reasons for escalations
- Review resolution times to determine the number of incidents the technical management teams are resolving within service level agreements (SLAs)

B.
- Obtain copies of available skills inventories and training plans
- Compare technology maintenance schedules with actual maintenance activities and the mean time between failure rates
- Review available project plans to ensure technical management is engaged early when new IT infrastructure components are being rolled out
- Review and assess the quality of technical documentation, including standard operating procedures (SOPs), system administration manuals and user manuals
- Contact the problem manager and determine whether technical management resources are contributing to the known error database (KEDB)

C.
- Conduct a skills inventory and training needs analysis and map the results to the service portfolio (if available)
- Review copies of maintenance schedules and project plans aimed at upgrading and maintaining the IT infrastructure
- Review technology performance metrics such as availability, utilization rates, and performance (e.g. response times)
- Review and assess the quality of technical documentation, including SOPs, system administration manuals and user manuals
- Review incident response and resolution times to determine the number of incidents resolved within SLAs

D.
- Review copies of available skills inventories, training plans and training records for each of the technical teams and for users, the service desk and other groups
- Review the technical management team's service operation process metrics and technology performance metrics
- Review copies of the availability and capacity plans along with available project plans
- Review change and release records and related deliverables such as known error entries
- Review and assess the quality of technical documentation, including SOPs, system administration manuals and user manuals

Question Seven

Refer to Scenario Seven

As an ITSM consultant, you have been asked to help write the functional specification for the toolset. The primary objective is to identify the functionality needed to satisfy the requirements for service operation, but also to consider any advantages that may be gained across the ITSM lifecycle.

Which one of the following options is the BEST summary of the high-level requirements for a toolset to support the organization's needs?

A.
- An integrated configuration management system (CMS) which allows all IT assets and relevant attributes to be held centrally, and which also allows relationships between each to be stored and maintained
- The capability to automate remote discovery of devices on the network and generate a report on discrepancies between deployments that have been discovered, and license details held within the CMS
- A workflow engine to improve the control of processes and automatically manage activities such as alerting and task escalation
- The capability to interface, manually and electronically, with tools used in other areas of the service lifecycle

B.
- An integrated CMS which allows all IT assets and relevant attributes to be held centrally, and allows relationships between each to be stored and maintained
- The capability to automate remote discovery of devices on the network and generate a report on discrepancies between deployments discovered and license details held within the CMS
- A menu-driven range of self-help facilities to simplify and improve the handling of service requests
- The ability to generate reports for use by other areas of ITSM

C.
- An integrated CMS which allows all IT assets and relevant attributes to be held centrally, and which also allows financial information about each asset to be stored and maintained
- The capability to input the findings from audits of the infrastructure and to report on numbers of licenses that are found as a result of the audit
- A workflow engine to improve the control of processes and automatically manage activities such as alerting and task escalation
- The ability to export data for use by other tools used in different teams

D.
- An integrated configuration management database (CMDB)
- Providing consistency with existing ways of working and other tools employed within the organization, in order to minimize the time taken to train existing employees
- Designing automatic import/export of existing information from other databases in the organization to allow continued use of, and minimum disruption to, existing working practices
- The ability for service desk analysts to take control of the user's desktop via remote control and thus to service any call through to resolution

Question Eight

Refer to Scenario Eight

Which one of the following options provides the BEST solution to address the concerns of this organization?

A.
- Create a common service operation activity of monitoring and control to support the availability and capacity management processes
- Redeploy technical staff to the operations bridge and train them to support the additional monitoring workload
- Once tools and staff are centralized, immediately evaluate tools and monitoring activities against both business and technical requirements
- Configure tools and procedures to meet the requirements of the availability and capacity management processes, in addition to the data already collected

B.
- Monitoring needs were developed by each group for specific operational purposes, so the associated monitoring and control activities should be retained within each IT department
- Availability and capacity management are not operational processes so a new set of requirements should be identified and documented
- Establish a team for availability and capacity management reporting to the A&P manager
- Define data input from operational departments and agree with the data centre to have reports submitted as required

C.
- Investigate and catalogue each department's monitoring requirements and tools used to collect report data
- Document both operational and non-operational needs for the capacity and availability management processes
- Establish a project team to analyse whether existing capacity and availability monitoring reports and tools can be utilized to meet new requirements
- Maximize cost savings not only by using the existing tools to meet the current monitoring needs, but also by expanding their use to meet new requirements

D.
- Initiate an organization-wide review of current monitoring and control capabilities, ensuring the involvement and support of the data centre manager
- Involve all departments in defining, agreeing, and executing processes and operational control procedures
- Ensure that monitoring and control is performed at all levels from component to service (including customer experience), to support the capacity and availability management processes
- Where possible, move routine monitoring and control activities to the operations bridge