ITIL® Intermediate Lifecycle Stream:

SERVICE OPERATION CERTIFICATE

Sample Paper 1, version 6.1

Gradient Style, Complex Multiple Choice

SCENARIO BOOKLET

This booklet contains the scenarios upon which the 8 examination questions will be based. All questions are contained within the Question Booklet and each question will clearly state the scenario to which the question relates. In order to answer each of the 8 questions, you will need to read the related scenario carefully.

On the basis of the information provided in the scenario, you will be required to select which of the four answer options provided (A, B, C or D) you believe to be the optimum answer. You may choose ONE answer only, and the Gradient Scoring system works as follows:

- If you select the CORRECT answer, you will be awarded 5 marks for the question
- If you select the SECOND BEST answer, you will be awarded 3 marks for the question
- If you select the THIRD BEST answer, you will be awarded 1 mark for the question
- If you select the DISTRACTER (the incorrect answer), you will receive no marks for the question

In order to pass this examination, you must achieve a total of 28 marks or more out of a maximum of 40 marks (70%).

Scenario One

A large financial institution relies on a number of IT services to support its business functions. Many of these are critical. Generally there is a good relationship between IT and the business, which has resulted in a reliable set of IT services that are aligned with the business needs.

The IT department has adopted ITIL and is seen as an example of best practice. Adopting ITIL has motivated the IT staff, who are keen to apply beneficial changes to working practices. The IT department has excellent service strategy and service design activities and processes in place. A well-managed service portfolio ensures that strong business cases are established for new and changed services. As a result, funding and other resources are matched to business and IT needs. Service level agreements (SLAs) are in place for all services.

The service desk is well managed and uses established incident management and problem management processes which are supported by a mature configuration management system (CMS) that incorporates a known error database (KEDB). These processes ensure that incidents and problems are escalated to the correct technical teams. This is essential as many services rely on specialist technology where only certain staff have the required skill to resolve issues. In general the service desk is well liked; however, there are some users who do not follow service desk procedures and who attempt to contact support staff directly or resolve issues without contacting IT. Requests from IT operations managers to business managers to ask users to adhere to service desk procedures have failed to bring about any change in the situation.

The technical management function is organized into a number of technology teams. Each team is well managed but service operation as a whole is a busy department. Staff are employed for their specialist skill sets, but because of the busy workload, little time is available for cross-training of roles or sharing knowledge.

Technical management teams use established monitoring and event management supported by associated tools. This provides access to much of the information that is used by other service management processes to report on various service levels. Service level achievements are good with very few major incidents or outages. Service availability targets are always met.

Scenario Two

An internal IT provider has developed its own applications for a number of years. Application development is carried out by a small team of developers. In general, the applications are considered to be successful by the business. The applications are well received by the users, who find them easy to use. In the past year, in order to meet the demands of the business, there has been an increase in the number of applications obtained from suppliers.

Six months ago, a new application management team was established as part of a service management improvement project. Generally, the two functions work well together and the combination of application development and application management has improved many areas. User acceptance testing has improved, with the result that common issues and defects are identified earlier in the life of applications and documented as known errors. Deployment activities have improved because application management, application development and IT operations management functions are involved in release and deployment tasks. Additionally, application management has implemented a policy that when applications are obtained from suppliers, appropriate support is included in the contract.

However, there are unresolved concerns over the day-to-day support of the applications.

The IT operations management teams find that they cannot deal with all the issues that arise. One result is that service level targets for restoration of service are not always met. When incidents occur, IT operations management can deal with the common errors but is unable to provide more specialist support. This is compounded by inconsistencies in the application architectures, platforms and development methods. This means that each application is different, thus making incident and problem diagnosis more difficult and time consuming. Further, when applications are implemented utilizing new technology the IT operations management teams do not receive the necessary training. An additional issue is that the number of incidents that are related to capacity and performance is increasing.

Scenario Three

A company has recently purchased a new event management support tool and the service operation team is in the process of installing and configuring the new tool. A question has arisen regarding the retention of data relating to events.

All of the people involved have agreed that events that are classified as warnings or exceptions need to be retained for a lengthy period after the event has been dealt with.

There are concerns regarding the amount of storage space that will be used and the sheer volume of data to be stored and potentially accessed. In response, some senior technical staff have proposed that events that are categorized as informational need only be retained for a minimal amount of time. A period of one week has been proposed, based on the assumption that if any follow-up issues have not occurred by then, they are extremely unlikely to occur at all.

Other team members have argued that this is inadequate. The data may be needed for some time beyond this point, so should be retained indefinitely.

A number of other requirements have emerged, which include the following:

- The organization's legal department has advised that there are legislative and compliance issues that require some data to be retained for up to six years
- There have been a number of serious IT security breaches that the IT security team claim could have been avoided if they had had access to a history of event data for all categories. The security management team wants relevant data to be retained for at least one year
- Problem management, capacity management and availability management have requested access to all event data to improve their trend analysis. All three have agreed to a retention period of six months

Scenario Four

A travel company with branches worldwide has a small number of geographically dispersed service desks that act as the focal point for a common incident management process. The service desks are quite well regarded but are only open during standard business hours (generally 08:00 to 18:00 with some local variations). The business has asked for support to be made available 24 hours a day, but cost constraints are currently preventing this.

A number of trends over the last few years have been identified:

- There has been a gradual increase in the total number of incidents handled
- An increasing percentage of the incidents handled are not, in fact, related to any sort of failure but are instead some form of service request from the users
- More than 60% of all incidents are now service requests of some sort
- There is some anecdotal evidence that higher priority failures are occasionally delayed or overlooked because of the volume of incidents and requests being handled at busy times

A high-level analysis of the service requests handled over the last six months reveals the following break-down:

Request Type	**Percentage**
Password change	35%
Additional mailbox space allocation	11%
Access to an existing application	9%
A new desktop application	7%
New user set-up	6%
Access for temporary staff/contractor	3%
Workstation move	3%
Other (various)	26%

Scenario Five

You are the recently appointed service desk manager of a national travel agency. The company has also appointed a problem manager. Both positions were created after a review of the IT department revealed that incident response times are failing to meet agreed targets. This is because the IT teams do not distinguish between incidents and problems and do not manage them separately. In some cases the result of this situation is that a service is not restored until IT has identified and implemented a full solution.

The review also identified the following:

- 25% of incidents are related to the main holiday booking service. This service is business critical
- 10% of incidents are related to the financial management service
- 40% of incidents are related to other services and general desktop issues
- 25% of incidents are categorized as service requests

The desktop incidents are a particular issue, as many seem to be recurring incidents and incur call-out charges from suppliers.

To address the issue, you and the problem manager are developing incident and problem management processes based upon ITIL guidance. Currently you are working on a program of training and awareness for service desk and technical support staff.

So far, you have agreed that:

- The service desk will log the call and seek a resolution if available
- Once the service is restored the service desk will check with the user and close the call if the user is satisfied.

Scenario Six

A regional utility company has a five-year strategy to grow the business and better serve its customers. In support of that strategy, it has acquired two local companies. One is a gas provider, the other an electricity provider. Part of the strategy is to quickly assess the technical management function in place at each company and determine how to best integrate the two companies.

You are a consultant and have been asked to develop a plan aimed at evaluating each acquired company's technical management function and assessing its abilities. Your plan is to benchmark each function against ITIL best practices in an effort to determine its current capabilities and level of maturity.

Your aim is to:

- Ensure the function is providing the organization with the technical knowledge and expertise needed to manage the IT infrastructure
- Determine whether the function is supporting the service lifecycle

Your first step is to collect and review the documentation being produced, in an effort to determine how effectively technical management is performing its role.

Scenario Seven

A large insurance company has recently identified the need to refresh the IT service management (ITSM) technology used to support the functions and processes within service operation. Organizational units have previously acquired or developed their own tools to meet specific requirements in their area, many of which are critical to the support of the IT services. This has led to an inconsistency in data and duplication of functionality throughout the organization.

Investigations have revealed that a lack of knowledge and understanding about the hardware and software assets exists across the organization and a particular vulnerability has been identified with respect to software licence compliance. The organization is looking for a toolset that will facilitate a solution to this particular problem without necessarily having to embark upon a full physical audit of their widely distributed infrastructure. The organization operates from a number of geographical locations, which are all connected via a reliable network.

The organization operates well-established processes but is keen to explore the benefits of adopting an ITSM lifecycle approach as recommended by ITIL guidance. Any new toolset must support the existing service management processes and improve communication within the IT functions.

Scenario Eight

The IT department of a company has implemented several ITIL processes over the past two years. Accomplishments in the ITSM program so far include:

- Improvement in incident and problem resolution rates
- Reduction in failed changes due to effective change planning and deployment
- High customer satisfaction as a result of negotiated service level agreements (SLAs) over two-thirds of business units

The IT group is organized into the following departments:

- Architecture and planning (A&P) – Managing key programs and setting standards for technology and processes
- IT control – Responsible for auditing and compliance against set standards and policies:
    - Service level management
    - Change management
- Data centre – Operational functions consisting of the following departments:
    - Operations bridge
    - Service desk
    - Mainframe management
    - Server management
    - Wide/Local area network management
    - Application support groups.

The data centre departments focus on managing their own technology, and usually communicate as required when an incident, problem or change is initiated. Each department is responsible for monitoring and controlling its own technology. Monitoring reports are generally circulated to each system administrator, and a summary of performance and exceptions is submitted to department heads each month. A monthly report on key system performance from each department is supplied to IT control and used to compile SLA compliance reports.

The organization is about to implement capacity and availability management processes. The project is being managed by the A&P manager. It is understood that the current approach to monitoring and control needs to change in order to address the requirements of these new processes. However, there is significant resistance from the data centre to allowing access to their data, or for any 'interference' in their monitoring activities or tools.