**Session 1: Event Management**

**1. What are the three types of events?**

Events in ITIL are classified into three types:

* Informational: Indicates normal operations, such as successful backups or service availability.
* Warning: Signals potential issues that may require attention, like high CPU usage or disk nearing capacity.
* Exception: Represents a deviation from normal operations, such as a service outage or hardware failure. These classifications help prioritize responses and ensure proactive monitoring.

**2. Describe the steps in the Event Management process**

Event Management involves:

1. Event Notification: Alerts generated by systems or applications.
2. Event Detection: Identifying events through monitoring tools.
3. Event Logging: Recording events for analysis and auditing.
4. Event Filtering and Correlation: Sorting relevant events and linking related ones.
5. Response: Automatic or manual actions to address the event.
6. Closure: Confirming resolution and updating records. This structured approach ensures timely detection and resolution.

**3. List commonly used tools/platforms that support Event Management**

Popular tools include:

* SolarWinds
* Nagios
* SCOM (System Center Operations Manager)
* Splunk
* Zabbix These platforms provide monitoring, alerting, and event correlation capabilities.

**4. Pick one and briefly describe how it handles events in an IT environment**

Splunk collects machine data from various sources, indexes it, and provides real-time analytics. It detects anomalies, correlates events, and triggers alerts for incidents. Splunk dashboards help visualize trends, enabling proactive management and quick troubleshooting.

**5. Explain how Event Management helps in early detection and minimizing service disruption**

Event Management enables continuous monitoring, allowing IT teams to detect issues before they escalate into major incidents. By identifying warnings and exceptions early, corrective actions can be taken promptly, reducing downtime and maintaining service continuity.

**6. Discuss the relationship between Event Management and Incident Management**

Event Management focuses on detecting and categorizing events, while Incident Management deals with resolving service disruptions. Events often trigger incidents; for example, an exception event like server failure becomes an incident requiring resolution. Together, they ensure operational stability.

**Incident Management**

**1. What is the purpose and goal of Incident Management?**

The goal is to restore normal service operation as quickly as possible and minimize business impact. It ensures user satisfaction and maintains agreed service levels.

**2. Incident Management Process Flow**

* Incident detection and logging
* Categorization and prioritization
* Investigation and diagnosis
* Resolution and recovery
* Closure and documentation

**3. Explain key aspects**

* Reporting: Via service desk or automated monitoring.
* Diagnosis: Root cause analysis and troubleshooting.
* Resolution: Applying fixes or workarounds.
* Communication: Regular updates to stakeholders.
* Time: Measured against SLAs.

**4. Mention KPIs**

* Average resolution time
* First-call resolution rate
* Number of incidents reopened
* SLA compliance percentage

**Session 2: Problem Management**

**1. Explain Reactive vs Proactive Problem Management**

* Reactive: Addresses problems after incidents occur.
* Proactive: Identifies and prevents potential issues before they cause incidents.

**2. Identify and eliminate root cause**

Problem Management aims to find underlying causes of recurring incidents and implement permanent fixes.

**3. Techniques for RCA**

* Fishbone Diagram
* 5 Whys
* Fault Tree Analysis

**4. Real-Life Scenario**

Example: Frequent network outages traced to faulty firmware. Solution: Upgrade firmware and implement monitoring.

**5. Contribution to CSI**

Problem Management reduces incident volume, improves reliability, and enhances customer satisfaction, supporting continual improvement.

**Change Management**

**1. Goal of Change Management**

To ensure changes are implemented with minimal risk and disruption to services.

**2. Process Steps**

* Request initiation
* Assessment and approval
* Planning and implementation
* Review and closure

**3. Firewall Update Example**

* Initiation: Change request logged in ITSM tool.
* Risks: Service downtime, misconfiguration.
* Mitigation: Backup configs, test in staging.
* Approval: CAB (Change Advisory Board).
* Implementation: Scheduled maintenance window.
* Review: Post-change validation and documentation.

**4. Unauthorized Changes Impact**

They can cause outages, security breaches, and compliance failures, severely affecting service availability.