**Session 1: Request Fulfilment**

**1. What is the purpose of the Request Fulfilment process?**

The purpose of Request Fulfilment is to manage and fulfill service requests from users efficiently. These requests typically include access to applications, hardware provisioning, or information. Unlike incidents, service requests are planned and non-disruptive. The process ensures timely delivery, maintains user satisfaction, and supports business continuity. By standardizing request handling, organizations reduce delays and improve transparency. Request Fulfilment also helps track approvals, monitor progress, and maintain compliance with organizational policies.

**2. Difference Between Incident and Service Request**

An **incident** refers to an unplanned interruption or degradation of a service that needs immediate resolution to restore normal operations. A **service request**, on the other hand, is a formal request for something new or additional, such as software installation or access rights. Incidents are reactive and urgent, while service requests are proactive and routine. Both processes aim to maintain service quality but differ in urgency and impact.

**3. Request Fulfilment Process Flow**

* **Request Logging:** User submits request via portal or service desk.
* **Approval:** Manager or system validates request.
* **Fulfilment:** IT team provisions requested service.
* **Closure:** Confirmation sent to user and record updated. This structured flow ensures accountability and timely delivery.

**4. Briefly explain how automation can improve Request Fulfilment**

Automation accelerates request handling by reducing manual intervention. For example, automated workflows can approve standard requests instantly, trigger provisioning scripts, and update records without human input. This minimizes delays, reduces errors, and improves user experience. Automation also enables self-service portals, allowing employees to fulfill common requests independently.

**5. Example: Employee joins and needs email, Teams, and printer access**

* **Request Submission:** HR raises request in ITSM tool during onboarding.
* **Approval:** Manager approves access based on role.
* **Fulfilment:** IT provisions email account, Teams license, and printer permissions.
* **Closure:** User receives confirmation, and request is marked complete. Automation can streamline this by linking HR systems with IT provisioning tools.

**Session 2: Access Management**

**1. What is the primary purpose of Access Management?**

Access Management ensures that authorized users can access services while preventing unauthorized access. It enforces security policies by granting, modifying, and revoking access rights based on roles and responsibilities. This process safeguards sensitive data and supports compliance with regulatory standards.

**2. Explain Access Management Process Flow**

* **Request Initiation:** User or manager submits access request.
* **Approval:** Verified by line manager or security team.
* **Provisioning:** Access granted using identity management tools.
* **Documentation:** Records updated for auditing.
* **Revocation:** Access removed when user leaves or changes roles. This structured approach ensures security and accountability.

**3. Example: New finance employee needs SAP, Outlook, and finance drive**

* **Request Raised:** HR or manager submits request in ITSM portal.
* **Approval:** Finance head validates need.
* **Provisioning:** IT grants SAP credentials, Outlook mailbox, and drive permissions.
* **Documentation:** Access logged for compliance.
* **Revocation:** Access removed during offboarding to prevent misuse.

**4. How Access Management aligns with Information Security Management?**

Access Management is a critical component of Information Security Management. It enforces confidentiality, integrity, and availability by ensuring only authorized individuals access sensitive resources. This alignment helps prevent data breaches, supports compliance, and mitigates risks associated with insider threats.