Question Bank for Interview

Incident Management

What is the scope of Incident Management ?

The Scope of the Incident Management Process can be defined on the basis of following standpoints such as:

a. Process Activities
b. Technologies / Applications Supported as an IT Service Provider
c. Locations Supported

Scope is explicitly defined in the Process document and varies from project to project. It provide clear distinction between what is In Scope and what is Out of Scope from a process standpoint

What are the steps you would follow as an Incident Manager when an Incident is reported or Describe the steps involved in Incident Management ?

As an Incident Manager we follow the following steps:

1. Incident Detection & Recording
2. Prioritization & Classification
3. Initial Support
4. Investigation & Diagnosis
5. Resolution & Recovery and
6. Incident Closure.

Define Incident

An Incident is an unplanned interruption to an IT Service or reduction in the quality of an IT Service.

The goal is to restore normal service operations as quickly as possible and to minimize the adverse impact on business operations, thus ensuring that the best possible levels of service quality and availability are maintained. Failure of a configuration item that has not yet impacted service is also an Incident.

In other words, an Incident is any event which is not part of the standard operation of service and which causes or may cause a disruption to IT Services or a reduction in the quality of IT Services

Walk me through the Lifecycle of a Critical Incident.

In my current organization, we follow the following steps:

1. Service Desk / Data Centre Operations or (via Event Monitoring) upon the detection of a Priority 1 / 2 Incident engages the Critical Incident Manager and Technical Support Group resources. Service Desk then open communication channels such as Email, and Instant Messaging are utilized to get inform the customer and internal stakeholders. Service Desk will open a Technical Bridge via MS Teams or Google Meet (depending on the project)

2. Escalation Procedures are followed to engage Backup Resources in case the Critical Incident Manager or the Technical Support Staff is not responding or unavailable.

3. Technical Bridge is used to provide a platform for Investigation & Diagnosis. This call is chaired by the Critical Incident Manager.

4. Critical Incident Notifications (Initial notification, hourly Updates, Resolution) are sent to the stakeholders at defined intervals by the Critical Incident Manager.

5. Once the Critical Incident is resolved, Major Incident Review meeting is scheduled by Critical Incident Manager and publish the MIR (Major Incident Report) with the internal and customer stakeholders

What is the difference between an Incident and a Service Request?

- An Incident is an unplanned event which causes or may cause Service Disruption or Performance Degradation example -- Application is not accessible by End User or multiple End Users

- A Service Request is a request from a User for information, or advice, or for a Standard Change or for Access to an IT Service example -- request for access to a file folder on SharePoint

How do you determine the effectiveness of the Incident Management process?

The effectiveness of the Incident Management Process can be ascertained by defining and reporting on Key Performance Indicators(KPIs) which are aligned to Critical Success factors. In my current organization we measure and report the following KPI's:

1. Number & Percentage of Incidents Resolved within agreed Service Levels (based on Priority).

2. Number & Percentage of Incidents Responded to within agreed Service Levels (based on Priority).

3. Mean Time to Resolve Incidents (MTTR) for each Incident Priority.

4. Number of Ageing Incidents.

5. Number of Reopened Incidents.

6. Average Customer Satisfaction Score.

7. Number & Percentage of Incidents Resolved at First Contact (FCR).

8. Percentage of Incidents that have Hopped (Reassigned) 3 or more times.

What ITSM Tools you have worked on ?

In my current / previous organization we use to work on ServiceNow and Remedy

Is the Known Error Database managed by the Incident Management Process? Or Who manages Known Error Database ?

Known Error Database is managed by the Problem Management Process.

What are the typical contents of a Major Incident Report?

In my current organization we use the following fields in the MIR Report:

1. Incident Number
2. Summary
3. Incident Detected Time
4. Incident Resolved Time
5. Business Impact
6. Affected CI
7. Chronological List of Activities performed to resolve the Incident
8. Root cause statement

Who can create or log an Incident?

Service Desk is the first point of contact for an End User, depending on the End User contact type an Incident can be created by:

1. Service Desk Agent for contact type as Email, Phone, Chat and Walkin’s
2. End User if Incident is reported via End User Portal

In some of the projects I have seen Email to ServiceNow integration and Incidents are created automatically when sent to Service Desk Inbox or Mailbox.

How can an Incident can be reported by an End User ?

An Incident can be reported by an End User via one of the following methods:

1. By sending email to Service Desk Inbox or Mailbox
2. By calling Service Desk
3. Via Support Chats
4. Via End User Portal
5. Via walk-ups to Service Desk area

What information is included at the time of creation of an Incident ?

Once the End User reports an incident, the service desk logs the incident. The incident should include information, such as but not limited to:

1.Name and Contact details of caller

2.Business Service

3.Configuration Item

4.Contact Type

5.Description of Incident

6.Categorization & Prioritization of an incident.

Explain Incident Categorization ?

Incident categorization is an important step in the Incident Management process.

Classification is required to categorize the Incident based on the Nature of the Issue and the Type of IT Component/Configuration Item that is affected. This enables:

1. Reliable Reporting and Analysis of Incidents to identify Trends and Patterns.

2. In ITSM Tool, Categorization involves assigning a Category and a Sub Category to the incident.

3. Auto Assignation of Incidents is done to the appropriate Support Group based on the impacted Configuration Item. On selection of Configuration Item (CI) Category, Sub-Category and Assignment Group is auto populated

Explain Incident Prioritization or Why should Incidents be Prioritized?

Incident prioritization is important for SLA response adherence.

The priority of an incident is determined by its impact on users or business and its urgency.

Priority is calculated according to Priority Matrix, formula = (Impact * Urgency) = Priority

In my current organization, Incident Priority is be based on the Impact and the Urgency associated with that Incident and criteria is based on:

1. The Tier of the Application/Infrastructure Element (Whether it’s Tier 1/2/3).
2. Number of Users Affected by the Incident.
3. Environment of the Affected Configuration Item (Production, Testing, QA etc).
4. Incident Reported by VIP Users.
5. Impact which differs on the basis of degradation in Performance, Partial Availability and Complete Outage.

Incidents is prioritized so that they receive the right amount of focus and resources necessary for that priority. It also helps in establishing the order of dealing with Incidents.

What is an Ageing Incident? How do you handle Ageing Incidents?

An Ageing Incident is an Open/Unresolved Incident which is open for a long time.
In my current / previous project we report aging of Incidents for:

1. Less than 5 days
2. 6 to 10 days
3. 10 to 20 days and
4. 20 + days

Ageing Incidents report is created on a daily basis and shared with Technical Leads and SDM during the Daily Service Review (DSR) call, this is then tracked and reviewed by the Support Group Leads to drive them towards closure.

When can Incident Record set to pending status?

It depends on the kind of agreement we have with the customer. An Incident can be put in pending status for one of the following reasons:

1. Pending Information from Customer

2. Pending Action by Customer

3. Pending Action by Vendor - In case Customer Managed Vendors (Vendor Ticket Number must be Referenced).

As soon as an Incident is set to pending status the SLA clock will pause. This will again depend on the agreement we have with the customer, I was part of one of the project where the SLA would never pause irrespective of the issue. We use to take exceptions for SLA’s not breached by us at the end of the month.

What is the difference between a Workaround and a Permanent Solution?

A Workaround is temporary fix that is deployed or executed to recover from an Incident whereas a Permanent Solution addresses the underlying cause to resolve the Incident.

Can an Incident become a Problem?

No, an Incident can never become a Problem.

Describe the role of the Service Desk

1. The Service Desk acts as a single point of contact mostly for Incidents and Service Request
2. Service Desk operates as per agreed business hours either from a single location or multiple locations
3. Incidents are accepted by one of the following ways but not limited to Web Interface (Self Service Portal), Telephone, Email, Chat Support
4. Support is provided to bonafide users only
5. Service Desk will create incidents and try to resolve L1 issues or issues which do not require L2 Support. They are often referred to as “First Level of Support”. Service Desk provides Incident Status to the customer throughout its lifecycle

Name types of Ticket Ownership

Ticket Ownership & Resolution Ownership

Ticket Ownership: In my current organization, Service Desk maintains the ownership of the Incidents until customer agrees that the Incident has been resolved.

Resolution Ownership: Typically it is with the Resolution Group to whom the Incident has been assigned.

The activities performed while providing incident resolution ticket is recorded in the Incident Ticket such as

Troubleshooting Steps, Reason for change of Assignment Group and finally the Resolution Notes

What do you mean by Response SLA and Resolution SLA?

- Response SLA is to capture the time taken by IT Support Staff to acknowledge a Ticket. It's calculated from Ticket Creation Time to ticket acknowledgement time (this is done via use of Status Codes in the ITSM tool).

  In other words, *Response SLA times usually refer to how quickly you will respond to a technical issue being raised via phone, email or other methods. In ServiceNow it stops when an Incident status or state is changed from “New to Assigned” and the “Assignee” field on the Incident Form is populated with the name of the person working on the Incident*

- Resolution SLA is to capture the time taken by IT Support Staff to resolve an Incident. it's calculated from Ticket submission time to time when ticket is moved to Resolution Stage (this is done via use of Status Codes in the Ticketing tool). Ticket Pending Time is excluded from this calculation.

  In other words, Resolution time is the amount of time between when the customer first opens a ticket and when that ticket is solved. In ServiceNow Resolution SLA *stops* when ticket is *closed*; *pauses* when ticket is *Pending Customer, Pending Vendor, or Resolved.*

How are SLA measured ?

SLA are measured by Priority – Four Priority levels is the most common that are defined in ITSM Tool like ServiceNow. It depends on the customer requirement as well. Priority levels are based on the incident’s business criticality – it’s Severity Level.

The SLA clock will pause once the resolution is provided or if an Incident status is set to pending. In case customer re-opens the Incident, the SLA clock will restart. However, the time between Incident resolution and customer rejection will not be counted for measurement of time taken to resolve the incident.

How do you handle tickets raised by or for VIP Users

We have a VIP Ticket Policy wherein all tickets raised by VIP users or on behalf of VIP Users will be automatically upgraded to have high urgency. Consequently, ticket priority will be suitably changed. For example if an Incident for an End User is raised as Priority 3, the same type of Incident for a VIP User will be created with Priority 2.

Can an End User reopen a resolved Incident ?

In my current project, An Incident can only be reopened by End User with a valid reason and is assigned to the last resolver Group.

Upon resolution of an Incident, End User receives an email with a link to either “Accept” or “Reject” the resolution provided by the Technical Team.

If the End User clicks on “Reject”, the Incident is reopened and is assigned to the last Resolver Group. In such case End User has to provide a proper justification / reason for rejection of resolution.

Under which scenarios can an Incident be cancelled ?

If a user needs a new service but reports it as an incident, tickets created by mistake, out of scope of IM Process should be cancelled and Ticket under the right process should be raised.

Explain different types of Escalation ? or How do manage escalations in your current organization ?

We have implemented an escalation matrix, there are 2 types.

Functional Escalation:

Transferring an incident from 1st level to 2nd level or to 3rd level support groups is called ‘functional escalation’ and primarily takes place because of lack of knowledge or expertise. Functional escalation also takes place when agreed time intervals elapse and must not exceed the (SLA) agreed resolution times.

1.to specialized skills for resolution

2. could be higher or lower in Organization

For example -- An Incident is logged by Service Desk, SD Agent does the initial troubleshooting for 15 minutes as part of L1 Support, if they are unable to resolve the Incident in a reasonable timeframe >> Incident is Transferred to Technical Support Group (L2 Support) for resolution.

Contd.. On next slide

Explain different types of Escalation ? or How do manage escalations in your current organization ?

Hierarchical Escalation (H): Hierarchical escalation' refers to informing or involving more senior levels of management to obtain management focus which can facilitate the resolution of the Incident. It should take place at any moment during the resolution process when it is likely that resolution of an incident will not be in time or satisfactory.

1.to senior level or authority

2.forewarning and awareness

3.requesting intervention

For example -- A Critical Incident is logged by Service Desk, SD Agent engages Critical Incident Manager and the Technical Support Group for speedy resolution of Incident. The Critical Incident Manager will review the SLA time left, in case determines that the Incident might not get resolved within the SLA or there is delay from Technical Support Group in joining the Technical Bridge call then Critical Incident Manager will escalate to Senior Management to create awareness and request for intervention to get the Critical Incident resolved

What is the difference between a Process and a Function?

A Process is a structured set of Activities designed to accomplish a specific Objective.

A Function is a team or group of people and the tools they use to carry out one or more Processes or Activities. For example the Service Desk.

Explain the interface between Incident & Configuration Management Process

The Configuration Management System (CMDB) is one of the primary sources of information for Incident Management and provides CI Attributes and Relationships to facilitate Incident Categorization, Prioritization and Resolution.

Define / Explain Problem

A Problem is the cause of one or more existing or potential Incidents. The cause is not usually known at the time a Problem Record is created, and the Problem Management Process is responsible for further investigation.