



6.2 Incident Management

Process Purpose / Objectives

The purpose of the Incident Management process is to restore normal service operation as quickly as possible and minimize the adverse impact on business operations, ensuring that agreed levels of service quality are maintained.

The objectives of the Incident Management process are to:

- Ensure that standardized methods and procedures are used for efficient and prompt response, analysis, documentation, ongoing management and reporting of incidents
- Increase visibility and communication of incidents to business and IT support staff
- Enhance business perception of IT through use of a professional approach in quickly resolving and communicating incidents when they occur
- Align Incident Management activities and priorities with those of the business
- Maintain user satisfaction with the quality of IT services

6.2.1 Assessment Score

- Maturity Score – 1.52 (Initial)
- Importance – 3.28

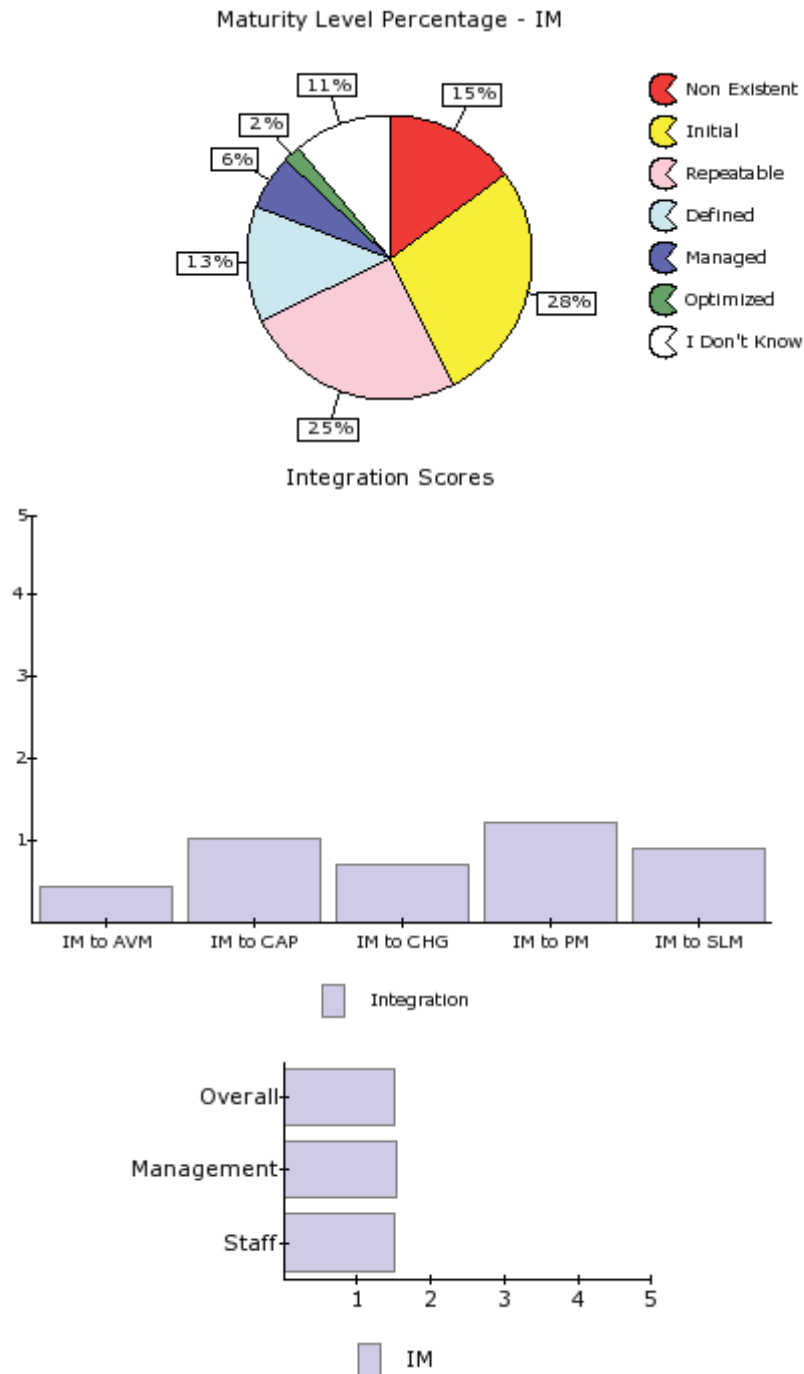


Figure 5 – Incident Management Scores



6.2.2 Observations and Conclusions

- This process ranked highest in maturity and is one of the processes that is followed relatively consistently (but not completely) across the enterprise
- The Incident Management Process Owner role is defined and assigned; the Process Owner seems to be known within the organization
- Incident Management process documentation includes a workflow diagram that clearly illustrates the Incident Management process as well as accompanying activity descriptions and roles
- The Support Center, the Single Point of Contact for users to contact IT staff, is not consistently used:
 - Users are sometimes encouraged to contact 2nd line staff directly
 - It is not uncommon for users to establish rapport with specific IT staff members who have provided good service in the past and use that IT staff as their primary point of contact
- Incidents can be assigned to technical groups responsible for the component that is affected based on information from monitoring tools
- There are multiple points of contact available to users depending on the nature of the issue and the service or resource being impacted by the incident
- Users may contact IT staff via email or phone and it is common for users to approach IT staff directly face-to-face. These incidents are initially assigned to a particular group based on point of contact
- Incidents are re-assigned (escalated) to another group if it is discovered that the issue lies in that technical domain
- Any practices related to an Incident Management process followed within different IT groups are not documented
- Specific functional group effort, knowledge and expertise are the determining factors in how an incident is handled
- The concept of ownership of an incident record throughout its lifecycle is not understood
- Specific IT staff members having ownership of incident resolution is a widely understood practice
- Reporting on the Incident Management process as a whole does not exist. There is no formal measurement and reporting in place



- Consistent and universally held process terminology and definition is not in evidence. There is no clear distinction between the definition of an incident, a problem and a service request. There are no universal terms for “User” or “Customer” as ITIL defines them
- Clear definition of incident prioritization and categorization models is lacking
- A defined measurement framework makes process improvement very difficult
- Overall, the approach to Incident Management is reactionary and based on individual expertise, commitment and cooperation rather than formally defined procedures
- There are no Service Level Agreements (SLAs) between OIT and its customers in support of Incident Management



6.2.3 Recommendations

- Define and implement a formal Incident Management process based on ITIL best practices. This includes documentation of procedures for handling all incidents according to a common categorization and prioritization model
- Clearly establish the Single Point of Contact for all users and define the procedures for initiating contact, the means of contact and the required responses to contacts from users
- Establish common terms and definitions related to Incident Management. In particular, the definition of what constitutes an Incident, a Service Request, a Problem and a Change need to be agreed and clearly documented and articulated to all UA IT staff
- Appoint the Support Center as owner of all incident records regardless of where it has been assigned in the organization. This single point of accountability for monitoring, managing, reporting and closing all incidents is a best practice approach that ensures all incidents can be effectively resolved, and improvements to the process more readily identified
- Establish process policies that define escalation and notification procedures and tie these to the prioritization and categorization models to ensure that timely and appropriate functional and hierarchical escalations occur
- Identify roles and responsibilities within all functional groups to act as Incident Analysts to ensure assignment of records and execution of incident investigation, diagnosis and resolution
- Expand on the current measuring and reporting functions around response times to include Incident Management process metrics, Critical Success Factors and Key Performance Indicators that are related directly to the objectives of the process
- Establish clear Incident Management policies where all inputs to Incident Management require an incident record to be opened in HP Service Manager regardless of where the incident is reported
- Require all OIT staff to follow Incident Management process and policies
- Establish metrics and reporting for the overall Incident Management process and activities. Cover not only basic Service Desk metrics about speed to answer and volumes, but also metrics that detail bottlenecks, and most frequent call types and errors to allow for trend analysis and ongoing improvement
- Configure HP Service Manager so incidents, service requests, problems and changes can be managed as separate record types which can be linked



- Establish a shared, easily searchable knowledgebase to improve the resolution of incidents and enable incident matching, allowing support staff to share knowledge between 2nd and 3rd level teams
- Develop the RACI (Responsible, Accountable, Consulted, Informed) Authority Matrix to clarify Incident Management roles and responsibilities, ensuring that all roles are well-defined, clear and aligned to OIT functional job descriptions and cross-functional organizational structure
- Develop a communication, escalation and notification model to provide clear guidance on communication based on priority level and potential time periods during the incident lifecycle (e.g. define the audience, method and notification time-trigger based on the incident priority). Where possible, automate these notifications as part of Service Level Management functionality within the tool
- Develop and provide training to all support levels to reinforce incident record update practices and procedures. Ensure the tiered support teams understand their role within the process and actively participate in incident record updates
- Consider the following Critical Success Factors to measure initial improvements:
 - Efficient Incident Resolution
 - This grounds any assertion that the Incident Management process provides value to individual users, and justifies the Incident Management process
 - Support Center is the Single Point of Contact (SPOC)
 - Incident Management communicates incident status through the Support Center
 - Required knowledge is shared
 - Incident Management shares incident data with support teams and the business to inform their continual improvement processes. Incident Management also solicits information from business units and support teams to better manage Known Errors and recurring incidents
 - Management commitment to Incident Management
 - Leadership plays a key role in setting the attitudes, behaviors and culture to achieve desired outcomes
- These Key Performance Indicators (KPIs) may provide the initial data points in support of the CSFs:
 - Reduce average resolution time
 - Increase percentage of incidents solved by the Support Center



- Reduce percentage of incidents initiated by end-users contacting support teams directly
- Reduce incident record quality issues
- Management is known to be a user of the Incident Management process