ITMM574 : Overview of Service Operation

Preethi Sethuragunathan A20387943

Illinois Institute of Technology, Chicago

Abstract

This paper present the overview of Service Operation, by detailing its Process and the stages that are involved in them. The main aim of the paper is to highlight the importance of service operation in the real time world and how interlinked its process are. Poor detection and deployment of Service operation results in unsuccessful IT models that fails to align with Business case and impact heavily on all aspects. Hence careful and detailed approach of Service operation is highly recommended as it can directly affect the organizational asset value , since this is the first stage of ITIL where the user see the changes by himself and a direct relation between the user and the business case starts here . To support this further, the paper discusses few published articles that analyzes in detail about the tasks and challenges involved in addressing each of the processes of the Service Operation specifically Incident, Problem and Access Management .

Keywords: Service operation, IT Models, Incident Management, Problem Management .

Overview Of Service Operation

Fourth phase of ITIL framework is the service operation .So far we have devised strategies, designed the business needs accordingly, imported necessary tools, calculated the changes with respect to the new business needs and now we are ready to see how well our changes have impacted the model.

Service operation is the phase where the actual changes are visible to the end user (customer /Client). From Every new changes such as renaming the project codes from characters to numeric in a IT company or re alignment of aisles in a super market or a new integrated support system to help online customers of a ecommerce website to the least - a new interior design in a chain of restaurants ,count as an outcome of Service operation . In a nut shell, this is the place where the Business analyst executes his input (ideas and methods so far implemented in the business case) to achieve the expected outcome. Additionally, refer the Figure 1 that shows how Service Operations blends the results of Transitional phase with the Continuous Maintenance.

Figure1: Roles of Service Operation

Objective:

From this, we can conclude that the main objective of service operation is to carry out all the activities such as taking care of agreements between the parties involved, changes suggested from the business, design and hardware perspectives from previous phases and make sure that all and every move with respect to the business goals are in compliance to the standards of ITM architecture.

Service: Why to use ?

Service Mgmt : How to Use

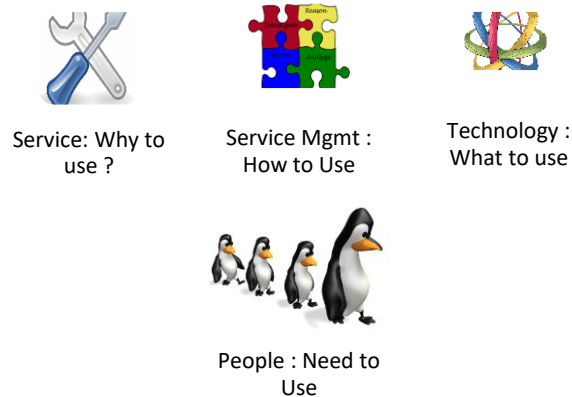Technology : What to use

People : Need to Use

Figure2 Scope of Service Operation

The scope can be summarized in 4 points: Service, Service Management, Technology and People, shown in Figure 2, above.

Service: Anything related to actual service comes under the scope. Be it an employer, employee, customer or owner or supplier, if you avail or offer a service, then all the process involved and related to such services can be accumulated under service operational scope.

Service Management: When we avail a service, then it needs to be well planned, designed and be presented for us to avail in the first place which is taken care of the service management. All controlling and managing factors comes are thoroughly detailed in this scope.

Technology: Today, no service exists without technology .That being said, choosing the right technology, applying necessary relevant tools that suits well to the business case is a challenging task which is discussed here.

People: All of the service, their management and technology that helped designing such services are aimed solely at people. Be it an end user or the service provider or the owner , People are the back bone of implementing any service and hence studying people , such as tracking patter behavior of user purchase on a e commerce website to feedback suggestion of a customer at a retailer store , or employee – company relationship programs in a company - building such related high end algorithms to monitor the changing mindsets of people are very helpful and often serves as the compass on where/why/need to drive pertaining to service operational issues

Consider this simple example of service operations in a leasing residential property:

A resident raising a maintenance request to the leasing owner on the resident portal.

Now, the resident portal is a technology tool that integrates the resident's issues/feedbacks/reviews to the owner. Whereas the owner can see a list of residents, administer their resident details, resolve the issues raised based on the priorities mentioned, react to the suggestions, and hence can manage all the resident related situations. Additionally an owner portal also manages the necessary relations with the maintenance team and the property welfare team ,performing legal process that are necessary to be completed to run the property , in relations with local police /watch force for better security on site .

So when a resident owner raise a maintenance repair request on a online tool, the owner receives it, generate a work order and delegate it to the maintenance team . The maintenance team now send a employee (handy man) to the field to repair, generate an invoice (free /charged service should be recorded) and submit to the maintenance management. Finally the owner closes the request by receiving the acknowledgement from the owner, employer and the maintenance team.

From this above example we can identify the important elements of the service operation, shown in Figure3
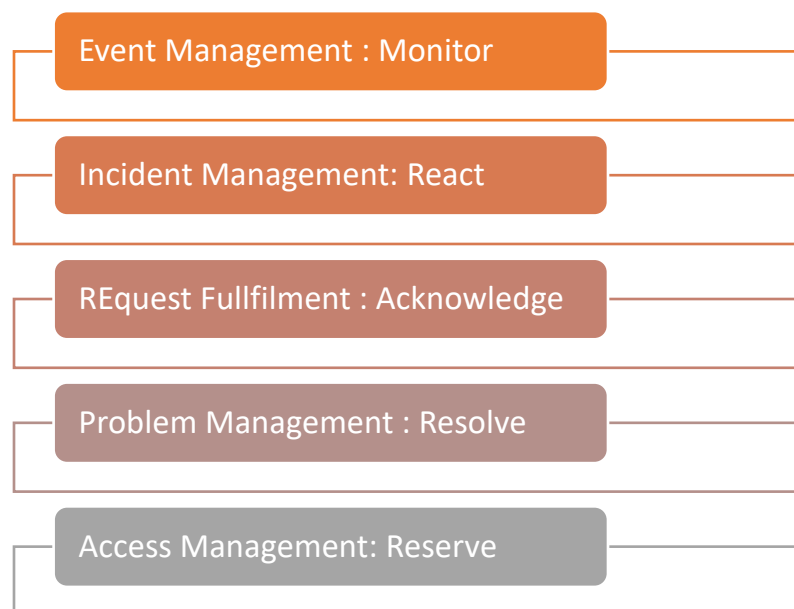
Event Management : Monitor

Incident Management: React

REquest Fullfilment : Acknowledge

Problem Management : Resolve

Access Management: Reserve

Figure 3 Process of Service Operation

1. Event Management:

The first and important process of the Service Operation is Event Management which monitors the activities happening in the 'system' thoroughly. Safety measures are seriously followed and unwanted behaviors are readily identified during this process. Activities that are enlisted in the Service Catalogue are checked then and to maintain the consistency and coordination with the business case as well the independent functioning of the activity .From a IT perspective , processes like tracking the usage of certain application/ or a server/ , monitoring the security of all the tasks performed in the bay , using tools to actively monitor tasks to be in compliance with security , taking actions about priority issues , maintaining the system , all covered under Event management . Typically an IT operation manager is the process head of this phase.

In our case, through online portal the owner handles, and overlook the activities happening in and around the residential site, taking appropriate actions, continual monitoring the site both physically and virtually (through the tool) .

2. Incident Management:

In this process, any unwanted behavior or simply a problem is detected and measures are taken to revert the issue to normal state. As unpredictable issues are almost rare, and Mostly the incidents that occur could be identified as a pattern, it's always a best practice to have a pre-defined 'to – do' things if being encountered with such kind of familiar incidents. For Example, a home LAN/ Broad band network experiencing a connectivity issue can be resolved by following a simple 'power cycling 'method that revives the network back to its normal workable condition. Hence it is important to case study a problem in detail and to come up with a 'to-do' model to revert the incident back. Such predefined steps are grouped as 'Incident Models' and they typically consists of following steps:

> *. What needs to be done with this exact error? Does this error /problem exists on its own or it reflects a problem of another activity.

> *. Priorities the steps one by one.

> * Are the steps needs to be taken to solve the issue lies within my privileges? If not who should solve this and how to contact them?

*.How much time is taken to apply the steps and how quickly it can resolve the issue?

*.Log the Incident thoroughly : Detection , Steps Taken , Time Consumed , Tools Used, Responsible persons to be tagged so that the incident itself serve as a case study for a future reference

After identifying and analyzing the steps above, the next is to examine the 'Incident' through the following stages of Incident Management:

- Logging: Documenting the incident, its nature of occurrence, when did the incident happen?
- Categorize: Organizing the incident depending upon its nature.
  Is it software or hardware issue? Or ecommerce issue?
  Categorizing helps to identify what kind of measures needs to be taken for particular incident.
- Diagnosis: Once categorized, list out the steps needs to be done in order to resolve.
- Prioritize: How important is the resolving of the issue? how dependent is the
  Issue with the other process?
- Escalate: Determining whether the process needs higher body escalation.
  Does it involve higher level access to detect the issue?
- Investigate: A complete analysis into the incident, preparing guidelines and
  Proper following of necessary steps
- Closure: Successful acknowledgement of issue resolving and documenting it.

In a typical IT environment, 'Service Desk' is responsible for performing all the activities and process involved in the incident Management. It is important to address here that identifying and determining the incidents are becoming increasingly challenging due to the huge amount of data involved. In a cluster of crucial data , to filter out the potential 'incident' possibilities is a number one goal of an Incident operation Manager and in a real time high end algorithms are effectively used to achieve the process . The main aim of the algorithm is to treat the big data accordingly thereby filtering out the more likely incident prone data out of the cluster. One such algorithm is discussed by the authors in the paper 'Big Data Architecture for IT Incident Management 'suggest

that MapReduce techniques to analyze the data and by using the NoSQL kind of databases to store the detected incidents . The authors also uses an proactive approach to track the independent components that are inevitably used in the It environment such as servers and network gears for incidents ,collect specific 'events' that trigger the standards in order to find the root cause of the incident .

Using this architectural approach, unstructured data can be formatted, categorized to highlight the alarming data that can be a potential risks are identified and then are analyzed. Through this paper the author also discusses about the significance of the Incident Management does affect the performance of the system as any late in the incident detection and resolving might actually impact the business case. Hence a quicker more efficient solution must be applied to restore the normal state of the system to assure its performance with minimal impact expected.

3. Request fulfillment:

Request Fulfillment is the process of managing the service requests that are raised from the users addressed directly to the Owner. Usually these requests are planned and can range from any information within to and pertaining the business environment like requesting details regarding a newly imported software or a tool or updating a password or information for a user account etc.

In our Example, the user creating a user account to raise a service request on the resident portal and the necessary follow up steps taken by the owner to fulfill the raised request denotes the process of request fulfillment

4. Problem Management:

In this process, the incidents that has the potential possibility of becoming a problem is identified, diagnosed and repaired successfully. The main objective of the Problem Management is to prevent the frequent occurrence of the incidents there by controlling the problem at the early stage. The first step of the process is to detect the problem , identify its root cause ,technically to be called as 'Known Error' which is then logged on to a separate file structure called Known Error Database .

Aspects:

Problem Management focuses on:

- How to identify an incident that could be a problem?

- How important is to determine the root cause of an incident /Problem?

- Prioritizing the steps to resolve the issue?

- How significant it is to refer the previous case scenario that are mostly /likely relevant to the current problem?

- Is it Possible for the problem to re appear, if so what needs to be done?

- Logging and proper documentation of the current problem for a future reference.

Process:

Problem Management is divided into two intrinsic process naming' Proactive & Reactive Problem Management'. As the name suggests, In the Proactive Process, steps to identify the root cause, precautionary measures to detect a problem, tracking frequent incidents are handled whereas in Reactive process, steps to do after encountering the particular problem are followed. That Said, the Problem Management goes through several stages similar to Incident Management that are listed as follows:

- Detection: Determine the issue, go through incident management.
    - Were the issue resolved properly in the previous stage?
    - What could possible cause the error?

- Logging :   Record /Document the problem : Divide and Conquer the Issue
    - Date and Time when the problem occurred.
    - At what stage the problem occurred?
    - Is it a problem on its own or a symptom of any other mishandled issue?

- Specification :Details of the Problem
    - Is it a Technical issue?
    - Can it be done within the provided access?
    - Does the issue resolving steps involve any higher escalations that needs notification in prior?

- Priority :
    - How important it is the problem to resolve?

- Can it resolve on its own like a system restart revival?
- If the problem solving helps to enhance the overall system or any late in the problem solving affects the overall performance of the system?
- How quickly and efficiently can the problem be resolved?

- Identifying Known Error :
  - Detect the Problem and documenting
  - Now that you know what the error is and list out the steps.
  - Are the steps feasible with respect to the current scenarios ?

- Resolve :
  - Fix the issue by following the steps mentioned.

- Closure: Successfully closing the issue after the repair and properly documenting it for the future reference.

Albeit, the real time problems of performing this particular process can be tricky as there are several methods in the market, each serving its own purpose. Hence to choose a problem management guidelines that suits our business case proves to be challenging and highly engaging task for which the author of the Paper ,'A conceptual Model for IT Problem Management'(2014) suggest a cumulative analysis of successive problem management models by different companies belonging to multifarious domains ranging from electrical to IT . The idea of the authors is to devise a design pattern to support their analysis of the cumulative approach that has been touched up by the software engineering aspects as well. The authors also successfully match the approach to that of testing and defect management, detailing testing techniques that could be deployed to effectively analyze the problem and to resolve it efficiently. Through this paper, we also understand that the problem management approach differ from company to company and it is important to be flexible and adoptive depending upon the individual requirements. Having strong base in ITIL standards with respect to service operation practices ,an IT analyst should run an end-end analysis on different kinds of available approaches to choose the most suitable and efficient one to get the desired result .

5. Access Management:

The last process of Service operation is the Access Management. Like the name implies, this process regulates who have access to problem and incidents let alone resolving the issue. This is an important process as it directly related to the security standards of an organization and deals with managing the sensitive and crucial data involved in and around the company. Through this process guidelines, system abuses can be easily identified in the incident Management process there by avoiding the system security and data theft threats at an early stage . Figure4 below shows the activities of Access Management.
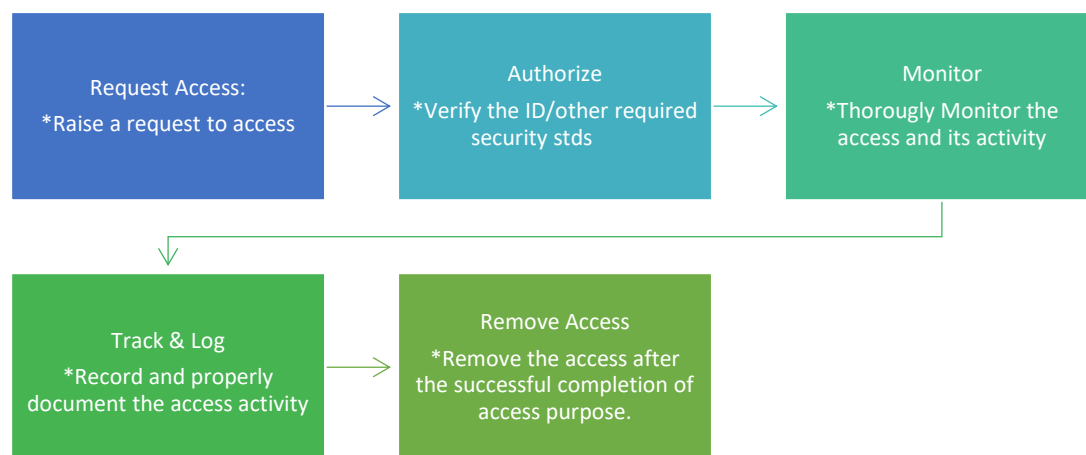
Request Access:	Authorize	Monitor
*Raise a request to access	*Verify the ID/other required security stds	*Thorougly Monitor the access and its activity

Track & Log	Remove Access
*Record and properly document the access activity	*Remove the access after the successful completion of access purpose.

Figure4: Activities of Access Management

Overall goal of the process it to provide the 'Right Access to Right Person' .On that key note, the role of Access Management concentrates on following criteria :

To determine who can access:

- Does providing access to this person /official / department help in repairing the process?
- How important is the access to the department?
- To determine any and all possibilities of security threats given the access to the department
- To establish strong security standards for the access. To establish request portals / formal ways to request an access.
- To prohibit shared access.

To determine who cannot access:

- Relate the issue with the user.

- Understand the administrative privileges.

- Understanding why there is limitations to the access.

Once the criteria is set and defined for the access, the process goes through a interlinked flow of activities within the process:

It is important to identify that in this internet era and high end data availability it is extremely tough to manage the security level tasks within the IT environment. If being careless, security breaches can seriously affect the business case and pertaining business tasks. The Article,' User Identity and Access Management Trends in IT infrastructure – an overview' discusses the above criteria in detail laying out the modern approaches that are in practice to verify and authorize users. Using authorization Techniques such as SSO, Web SEAL that provide user provisioning systems user credentials are easily managed .The research also gave away innovative functions to reverse engineer the access and identity management based on security standards. By studying the overview of Federated Identity Manager, the challenges and Risks involved in the IT security systems are readily understood.

Conclusion:

Thus, careful and detailed deployment of Service Operation and its process are extremely important and as mentioned and discussed, following suitable algorithms and best industrial approach, it becomes easier to surpass the potential threats that are expected in this process which in turn assure the consistency and overall performance of the system.

References

Liu.R ; Li.Q ; Li.F ;Ljuen .M ; Juhnyoung .L. (2014). Big Data Architecture for IT Incident
Management. *IEEE Conference Publications* , Vol#(Issue#), Page numbers 424-
429.doi:10.1109/SOLI.2014.6960972

Mark .J ; Anne .E ; (2006). A conceptual Model of IT Service Problem Management . *IEEE
Conference Publications. International Conference on Service Systems & Service
Management.* Pages 798-803 doi: 10.1109/ICSSM.2006.320564

Manav.A,Thakur ; Rahul.G . (2015).User Identity and Access Management trends in IT
Infrastructure – an Overview. *IEEE Conference Publications. Pervasive
Computing(ICPC) International Conference.* Vol#(Issue#), Pages 1-4.doi:
10.1109/PERVASIVE.2015.7086972