ISSN:0975-9646



# Incident Management & Service Level Agreement: An Optimistic Approach

Bilas Ghosh

*Department of Computer Science and Engineering*
*Vellore Institute of Technology, Vellore, India*

***Abstract*** **- In our increasingly complicated and distributed world, Incident management and Service level agreements (SLAs) are becoming a very critical tool for defining, measuring and managing the performance of services that comprise our companies. Whether an organization is a provider or consumer of services, stronger service level management leads to better service and lower costs. Yet most companies are less than satisfied with the business value they receive from their SLAs as well as the time and cost of monitoring and administering those agreements. This paper is intended to help IT organizations gain greater value from their Incident Management & SLA management efforts.**

***Keywords*****— Incident management, SLA, Problem ticket, Change request, alert threshold, warning threshold, SLM, RCA.**

## I. INTRODUCTION

The primary goal of the Incident Management process is to restore normal service operation as quickly as possible and minimize the adverse impact on business operations, thus ensuring that the best possible levels of service quality and availability are maintained. 'Normal service operation' is defined here as service operation within SLA limits. The role of an SLA is to clearly define service delivery expectations, provide an objective means of assessing whether performance meets those expectations and identify the actions needed to improve performance. This role is crucial in today's business environment where an interrelated web of companies receives and provides services to each other. Our suppliers' performance affects our performance, which in turn affects the performance of our customers. If our performance falters, our customers can find plenty of competitors willing to take our place. In this light, it is easy to see the strategic advantage of well-tuned SLAs.

## II. FIRST THINGS FIRST – WHAT IS INCIDENT

### *A. Incident*

An incident is an unplanned interruption to an IT Service or reduction in the Quality of an IT Service. An incident occurs when the operational status of a production item changes from working to failing or about to fail, resulting in a condition in which the item is not functioning as it was designed or implemented. The resolution for an incident involves implementing a repair to restore the item to its original state.

Few key points about solving Incidents which has to be kept in mind are:-

- Incidents are properly logged
- Incidents are properly routed
- Incident status is accurately reported
- Incidents are properly prioritized and handled in the appropriate sequence
- Resolution provided meets the requirements of the SLA for the customer.

## III. INCIDENT MANAGEMENT PROCESS

This process should be used whenever an issue is reported where there is a loss of service or lack of service. For example, an user that receives an error message when trying to run an application, or automated alert got raised when automation process failed to build something which customer has ordered (e.g. building a VM for a customer by cloning from pre-defined template)

### *A. Incident Raised*

This is the state that a new ticket starts when information regarding the Incident is entered.

### *B. Incident routed to appropriate support team*

This is the starting point for all incident tickets after they have been submitted. Tickets are submitted to either a queue which will be accessible to all members of the support group or directly to an individual based on definable auto-routing criteria. The auto-routing feature allows tickets to be directly routed to a SME (subject matter expert) based on requirement.

### *C. Level 1 (L1)*

A support group folder may be the first owner for new tickets and a team member will be responsible for any unassigned tickets in this state. They will be investigating the Incident themselves to resolve it. If it is out of scope for them (the error is not in the KEDB and has no resolution), they have the option of forwarding it to a more qualified member of the support team (Level 2) if this would be more efficient.

Before forwarding to Level 2 team, the following information regarding the Incident should be entered by Level 1 team members:

- Description of the issues
- Any troubleshooting activities they have performed
- Any other observations made.
- Urgency of the issue

*D. Level 2 (L2)*

An incident in this state has had initial investigation and troubleshooting performed without success. There are no documented processes to resolve the Incident or those processes have been attempted without success. A team member from L2 should investigate and resolve this issue.

*E. Raise Problem Record*

If the Level 2 support person identifies a problem and thinks that a change to a configuration item is necessary to resolve the incident, he should first raise a problem ticket. Performing the "Report Problem" action will move the incident to the "Under Investigation" state and a new problem record that is linked to the initial incident record should be raised.

*F. Raise Change Record*

This is performed when the Level 2 support person identifies that a change to a configuration item is necessary to resolve the incident.

*G. Change Implemented / Completed*

After the change has be implemented successfully it would resolve the incident. Now it requires attention from the support person responsible for the ticket. This may simply mean contacting the incident submitter to verify that that their issue has been resolved or may involve additional troubleshooting steps to complete required work.

*H. Incident Resolved*

This action is performed when the support team (either L1 or L2, as reuired depending on the issue) is able to restore service to the customer either using known steps or through investigation and troubleshooting.

*I. Inform Customer/User*

The support person should inform and verify with the customer that they have resolved the issue.

*J. Close Incident Ticket*

Once the incident has been resolved, it should be closed with proper closure code.

*K. Get RCA & Update Knowledge Base*

After the incident is resolved, root cause of issue should be investigated, and knowledge database should be update for future reference.

*L. Close Change Record / Close Problem Record:*

If a problem record and change record was opened to resolve the incident, these should also be closed with proper resolution code.

The whole process (Incident Management Process) is explained using flowchart in the next page of this document.

'Red' colour line indicates that the process is followed only when Problem record or change record is raised, otherwise not.

'Dotted' line indicates that the incident ticket is linked with problem record.

## IV. Resolving Incidents

Below process describes the basic structure of what actually needs to resolve an incident:

**Inputs:** The necessary information's required by 'Functional Group' to solve the issue.

**Functional Groups:** It consists of the relevant teams involved to resolve the issue.

**Output:** When issue is resolved the information given out by the 'Functional Groups'.

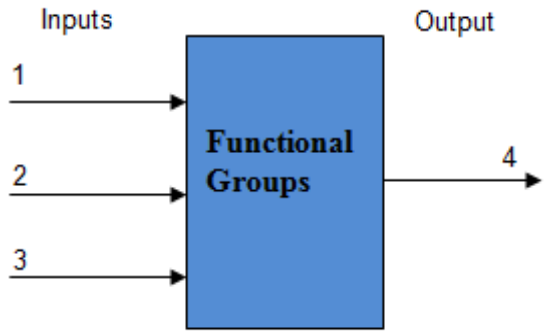



Fig. 1 Structure of resolving Incidents

The points mentioned in the above process are defined below as indicated:

Inputs:

1. Incident Number: This is the number generated when an issue is logged / reported in the platform.

2. Issue faced by customer / end user, observations.

3. Other necessary Technical Details required in solving the issue.

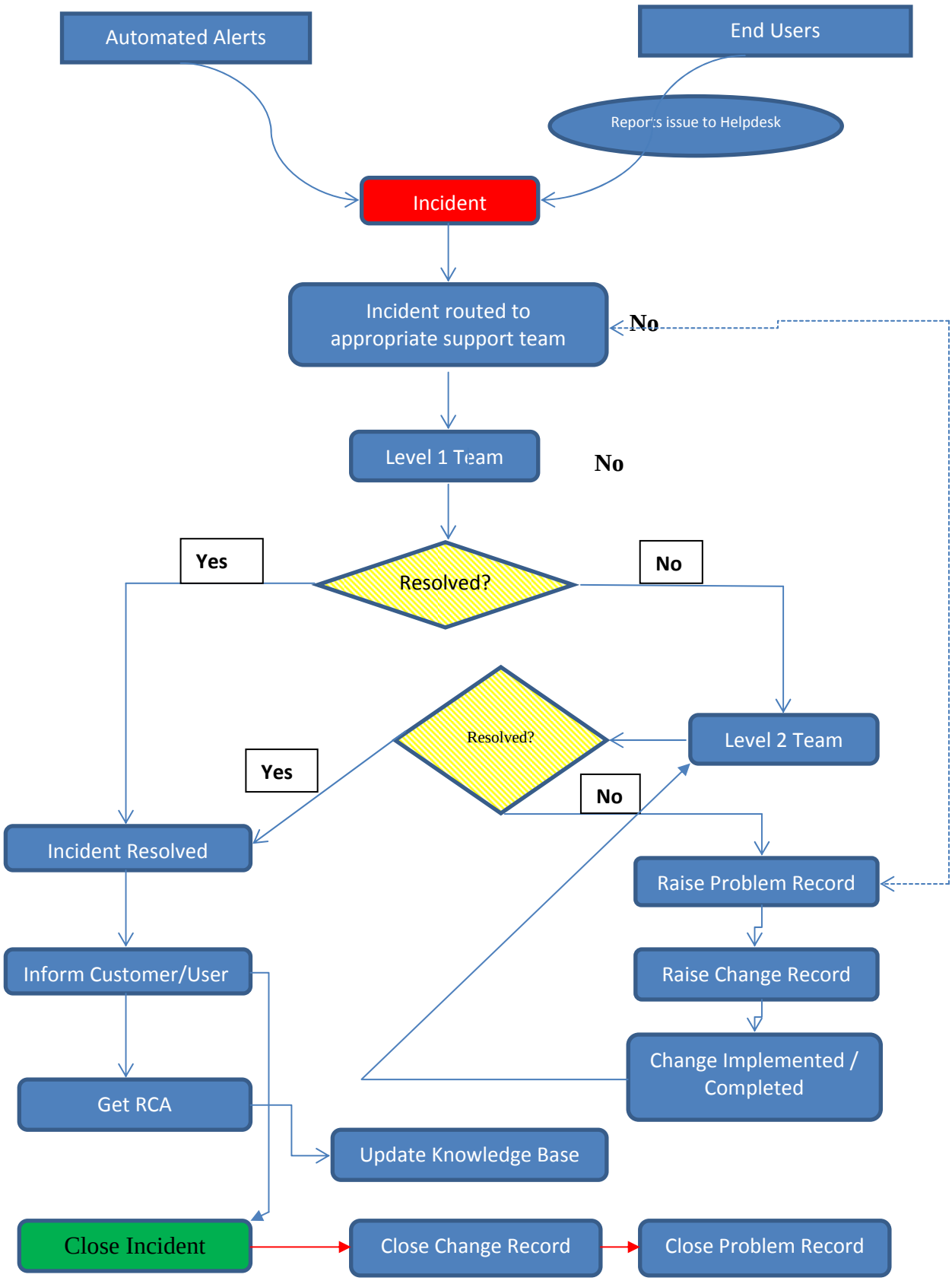
Output:

4. Standard notification to the customer when issues are resolved and case is closed.

## V. Service Level Agreement

Here we will just describe what SLA is and how SLA is decided for different priorities of incident tickets. A Service Level Agreement is two things: a negotiation tool to balance the user demands against the resources available. After this negotiation is complete the SLA serves as the definition of reasonability. For example, it may or may not be reasonable for an end-user to demand you maintain backups for 5 years, depending on the SLA. In absence of an SLA, it is possible for you to be held accountable for NOT maintaining that backup for 5 years - not because you should have, but because the fact that you don't/ wasn't known, agreed to, or communicated.

**INCIDENT MANAGEMENT PROCESS FLOWCHART**



*A. SLA*

A Service Level Agreement (SLA) is a contract between Service Providers or between Service Providers and Customers that specifies, usually in measurable terms, what services the Service Provider will furnish and what penalties the Service Provider will pay if he cannot meet the committed goals. The SLA will drive Service Provider differentiation during the exploitation (contributing to this customers trust) in terms of managed reliability and monitoring capabilities.

*B. SLA Matrices for different Priority Incidents*

Below are the three metrics for determining the order in which incidents are processed:

1. **Impact** - The effect on business that an incident has.
2. **Urgency** - The extent to which the incident's resolution can bear delay.
3. **Priority** - How quickly the service desk should address the incident.

Priority of incidents should be made dependent on Impact and Urgency. Priority is generated from Urgency and Impact.

Below table shows the priority of incident tickets when Impact & Urgency varies from High to Low.

TABLE I
IMPACT VS. URGENCY VS. PRIORITY

| Impact | Urgency | Priority |
|---|---|---|
| 1 - High | 1 – High | 1 - Critical |
| 1 – High | 2 - Medium | 2 – High |
| 1 - High | 3 - Low | 3 - Moderate |
| 2 - Medium | 1 – High | 2 – High |
| 2 – Medium | 2 – Medium | 3 – Moderate |
| 2 - Medium | 3 – Low | 4 - Low |
| 3 - Low | 1 – High | 3 - Moderate |
| 3 – Low | 2 – Medium | 4 – Low |
| 3 - Low | 3 – Low | 4 - Low |

Based on the above criteria we have prepared the SLA compliance report which we have met in last four quarters of a financial year (Q1, Q2, Q3, Q4) for 'Incident' tickets and 'Change' records.

P1 – Priority 1 incident tickets (Critical)
P2 – Priority 2 incident tickets (High)
P3 – Priority 3 incident tickets (Moderate)
P4 – Priority 4 incident tickets (Low)
SLA success rate is given as percentage.

'Red' colour indicates that we have failed to achieve SLA cut-off in that particular period. 'Green' colour indicates that we have successfully achieved SLA cut-off in that particular period.
We have also given the volume of incident tickets (in numbers) generated during each quarter, and also the number of 'Changes' implemented in each quarter.
'NA' represents that SLA calculation was not done for a particular priority of ticket in a period, since no tickets of that particular priority generated during that time.

| SLA Compliance report for <Client Name> | | | | | |
|---|---|---|---|---|---|
| Incidents | Targets | Q1 | Q2 | Q3 | Q4 |
| Incidents | | | | | |
| P1 SLA Success (%) | 80 | 80 | 82 | 100 | NA |
| P2 SLA Success (%) | 78 | 84 | 100 | 100 | 100 |
| P3 SLA Success (%) | 82 | 78 | 98 | 100 | 98 |
| P4 SLA Success (%) | 95 | 96 | 100 | 57 | 100 |
| P1 Ticket Volume | | 5 | 8 | 4 | 0 |
| P2 Ticket Volume | | 19 | 7 | 17 | 5 |
| P3 Ticket Volume | | 264 | 125 | 148 | 101 |
| P4 Ticket Volume | | 62 | 9 | 7 | 3 |
| | | | | | |
| Changes (CR) | | | | | |
| % SLA Success | 98.5 | 100 | 100 | 100 | 100 |
| Volumes | | 5 | 6 | 3 | 2 |

Fig. 2 SLA Compliance report generation and incident volume

## VI. PROPOSED WORK ON IMPROVING SLA

It has been observed that SLA of a whole platform or application breaches due to the incident tickets which gets generated due to 'capacity' issues. Here I would be discussing on how to improve SLA for these types of incident tickets and the process followed to do so.

In many cases it has been observed that automatic alerts (in the form of incident cases) have been set when resource utilization crosses a pre-defined threshold. It is a good practice, but few points can be modified (in terms of getting automatic incident tickets getting raised) which will give a better SLA. This method is taken into account since a lot of incident tickets get raised due to capacity issues in Production Platform of any IT project.

*A. Few points to note for older process*

1. Tickets getting generated when Resource Utilization >= Warning Threshold
2. Tickets getting generated when Resource Utilization >= Alert Threshold
3. Now it is observed in above 2 points that TWO tickets are getting raised simultaneously and at the same time when

Resource Utilization >= Alert Threshold - one for breaking
'Warning' and another for breaking 'Alert Threshold'.

*B. New proposed Process Algorithm*

**If** ('Resource Utilisation Percentage' >= 'Warning Threshold' & 'Resource Utilisation Percentage' < 'Alert Threshold') **then**
Send email notification to Capacity Mgmt. Team

**Else** (Resource Utilization >= Alert Threshold) **then**
'Generate Incident case with Capacity Mgmt. Team' & 'Send email notification to Capacity Mgmt. Team'

The following observations can be deduced from the above process:-

1. Ticket should only be generated only when the below rule is satisfied:

**'Resource Utilisation Percentage' IS GREATED THAN 'Alert Threshold'**

2. Tickets SHOULD NOT be generated for the below rule:

**'Resource Utilisation Percentage' >= Warning Threshold**

3. ALERT MAILS will be generated when the below rules are satisfied:

**'Resource Utilisation Percentage' >= Warning Threshold**

**'Resource Utilisation Percentage' >= Alert Threshold**

*C. Benefits of above 'New' process*

- Reduction in generation of un-necessary duplicate incident tickets for same issue. This also benefits in Incident Management process.
- It is always easy to manage SLA for lesser number of incident tickets than a huge number of tickets for the same issue.
- Capacity mgmt. team will directly get an automated mail in their inbox to act on les critical issue (when resource utilization only crosses 'Warning' threshold.)

We made a comparative study using the old process and new process of managing 'Capacity' related incident tickets as presented in the below tables. 'New' process was introduced in the month of December.

TABLE III
FOLLOWING 'OLD' PROCESS

| Month | No. of incident (2)* | No. of incident (3)# | SLA breach (4)* | SLA breach (5)# |
|---|---|---|---|---|
| June | 32 | 2 | 25 | 0 |
| July | 43 | 5 | 34 | 1 |
| Aug' | 28 | 0 | 22 | 0 |
| Sep' | 37 | 3 | 31 | 0 |
| Oct' | 31 | 5 | 23 | 2 |
| Nov' | 47 | 4 | 35 | 0 |

TABLE IV
FOLLOWING 'NEW' PROCESS

| | No. of mails (6)* | No. of incident (3)# | SLA breach (4)* | SLA breach (5)# |
|---|---|---|---|---|
| Dec' | 35 | 3 | 0 | 2 |
| Jan' | 32 | 3 | 0 | 1 |
| Feb' | 39 | 4 | 0 | 1 |
| Mar' | 43 | 2 | 0 | 0 |
| Apr' | 24 | 1 | 0 | 1 |
| May | 38 | 2 | 0 | 1 |

Where:-

(2)* - No. of incidents got raised when 'Resource Utilisation' >= Warning Threshold

(3)# - No. of incidents got raised when 'Resource Utilisation' >= Alert Threshold

(4)* - SLA breached when 'Resource Utilisation' >= Warning Threshold

(5)# - SLA breached when 'Resource Utilisation' >= Alert Threshold

(6)* - No. of automated mails got sent to Capacity Mgmt. team when 'Resource Utilisation' >= 'Warning Threshold'.

We have tabulated the above data in bar chart and represented the performance. Data of Table II is tabulated in Fig 3.

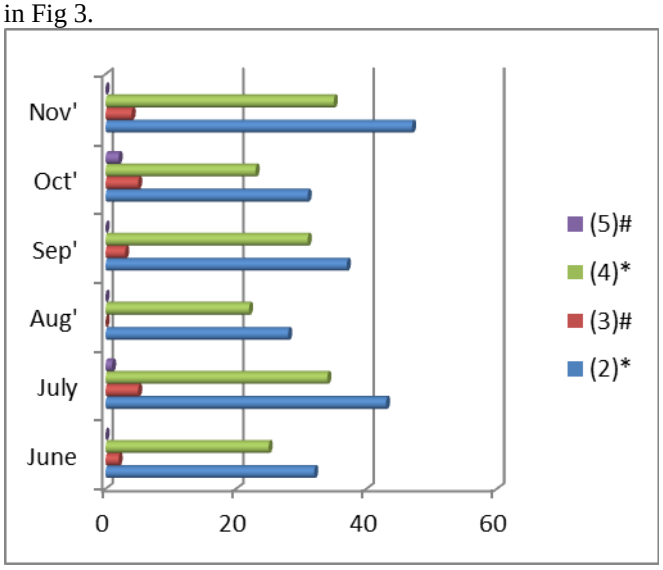



Fig. 3 Performance using 'Old' process

Data of Table III is tabulated in Fig 4.

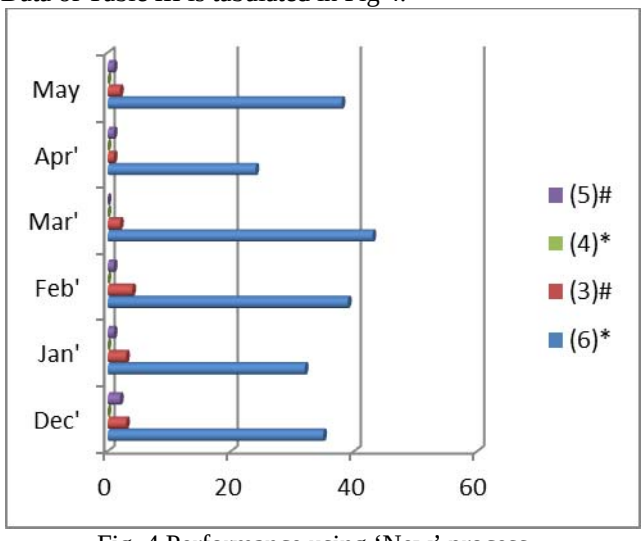



Fig. 4 Performance using 'New' process

So from here we can see that SLA performance and Incident management got bettered by a huge margin, when we followed the 'New' process.

This process requires only one commitment from capacity mgmt. team is to read mails more seriously.

## VII. CONCLUSIONS

Whether one's organization is a service provider or a service recipient, implementing effective service level management will pay back in terms of better service and improved business performance. Well-designed SLAs and strong service level management applications and processes reduce the time and effort needed to administer agreements, provide better and more timely information, lead to fewer service problems and faster resolution when problems occur, and last but not the lease result in stronger long-term relationships between suppliers and recipients.

## REFERENCES

[1] Meesters, Barry J.M.A. and Bouman, Jan F, 2000, *World Class IT Service Management Guide 2000, Article: A Service Check, ten Hagen & Stam Publishers (NL)*

[2] ITIL Service Delivery, Version 3.0, Draft for QA, November 2000, Central Computer and Telecommunications Agency (CCTA) (UK)

[3] ISO 9001:2000 standards, Quality management systems – Requirements (6WDJH GDWH: 2000-12-08), International Standardization Organization (ISO), Geneva, (CH), Link: http://www.iso.ch/

[4] *"SLA Management Handbook"*, -TMF GB971-, June 2001.

[5] Gerard Blokdijk and Ivanka Menken, *The Service Level Agreement SLA Guide - SLA Book*, 2008

[6] J Desai , *Service Level Agreements: A Legal and Practical Guide*, 2010

[7] G. Desoblin, H. Papini, *"SLA management: a key differentiator for service providers"*, 3rd quarter 2001.