Technical document

Incident Management System

**Submitted By**

Rajesh Kumar

Contents

[1. Introduction 2](#_Toc62506873)

[1.2. Reasons for selecting the subject area AND DATA 2](#_Toc62506874)

[1.3. Vision and Goals 2](#_Toc62506875)

[1.4. Key StakeHolders 2](#_Toc62506876)

[2. SCHEMA 3](#_Toc62506877)

[3. ETL 3](#_Toc62506878)

[3.1 Implementation 4](#_Toc62506879)

[3.1.1 Staging data mapping etl 5](#_Toc62506880)

[3.1.2 Data Warehouse ETL 5](#_Toc62506881)

[4. VISUALIZATIONS AND REPORTS 8](#_Toc62506882)

[4.1. Visualizations 8](#_Toc62506883)

[Categories wise Incident 8](#_Toc62506884)

[Priority Incident Count 8](#_Toc62506885)

[Total Reassignment 9](#_Toc62506886)

[Average Closing time 9](#_Toc62506887)

[Dashboard 10](#_Toc62506888)

[4.2. SSRS Reports / Visualization 10](#_Toc62506889)

[Yearly incident count 10](#_Toc62506890)

[Yearly Detailed Report 11](#_Toc62506891)

[Service Level Agreement(SLA) 11](#_Toc62506892)

[Priority Overview and detailed 12](#_Toc62506893)

[6. Conclusions 13](#_Toc62506894)

[7. Bibliography 13](#_Toc62506895)

[Appendix A – VISUALIZATIONS Code 13](#_Toc62506896)

# 1. Introduction

The principal motivation behind the Incident management system is to provide knowledge about technical incidents/issues, Bug generated in the field of Information technology in the year 2016-2017. It is nothing but the processing activity of an Information Technologies organization to analyze, identify, and fix the issue as well as to prevent a similar kind of issue in the future. The Source Data has been extracted from the service Now for the year 2016-2017 (Amaral & M., n.d.). The incidents are divided into three categories based on their priority namely Low, Medium, and High, Critical. Each priority defines the impact of the incident on the company and thereby defining the urgency of solving the issue. Each incident has an open date (the date when the incident was generated), closed date (the date when the incident was resolved), the impact of the issue, the urgency of solving the problem, and the priority required to solve the incident. This data is collected for an audit system for an instance of ServiceNow for the year 2016 (Amaral & M., n.d.). and the dataset can be found and downloaded from the URL

<https://archive.ics.uci.edu/ml/datasets/Incident+management+process+enriched+event+log>.

## 1.2. Reasons for selecting the subject area AND DATA

Most of the Information Technologies / Financial Services company usually faces throughout the year is an issue related to their system/Data/loading process, etc. These kinds of issue data logs can be used to understand patterns related to the incidents generated thereby coming up with better solutions to deal with these redundancies. Without an appropriate occurrence arrangement of Incident administration, the episode can upset the business activity, a whole group, worker, clients, business clients, or the whole capacity of the business. Therefore, the Incident Management process is very important in limiting the disruption caused by such kind of an event and run the business as usual.

## 1.3. Vision and Goals

The main objective is to help the Information Technologies company to minimize the time taken for an incident and reduce the completion time and effort to minimize the resolution cost and Service level Agreement (SLA) breech.

Below Objectives and overall metric also considered for efficient Incident Management and resolution performance:

* Reduce Completion time
* Fast and Easy identification of Issue caused
* Accurate Assignment group
* Avoid /Less Repetitive Incident
* Low attrition rate

## 1.4. Key StakeHolders

The Primary Stakeholders in these cases are Financial Services companies /Information Services Companies Clusters lead, change managers, Business Users, and a group of internal/external stakeholders who are involved in the economic transaction as well as the internal and external clients /executives.

# 2. SCHEMA

Diagram

Description automatically generated

Star scheme is used for defining the data model for the selected dataset for the best modeling approach highly adopted by relational data warehouses. Star schema is divided into two types of tables i.e. Dimension and Fact tables.

Using the multidimensional approach, we first defined the dimension table such as **Incident** **Dimension**, **Category** **Dimension**, **Date** **Dimension**. In the further investigation and identifying unique values in the incident dimension, we come up with further dimensions such as **Status** **Dimension** and **Priority** **Dimension**.

Fact table **Fact\_Incident** created and designed to store the effect of the incident in the time frame. Some of the attributes needed in the fact table, and ready for aggregation by the user’s business requirements.

# 3. ETL

ETL is nothing but the process of Data Integration process referring to three different stages as Extract, Transform, and Load. ETL is used to extract the data from various/different source systems and then transform the data based on the business rules, calculations, and finally load the data into the warehouse database system. Once published into the Datawarehouse and data-mart database then it's getting visualize using the visualization tools such as SSRS, SQL queries, Tableau, Excel, etc. by the end-users. The generic ETL Architecture of Datawarehouse is given below (Javapoint, n.d.):

Diagram

Description automatically generated

## 3.1 Implementation

**Data Analysis**

The dataset contains 141.7K incident events for 24K incidents, followed by 36 column attributes. The incident management process exercise to organize the column into below four categories:

* Incident reported by customers
* Information provided related to system
* Processing incident
* Close Incident

**Missing Value**

In the overall dataset, 17.53 % of data values are missing, to the void of information some of the missing cells were removed and some cells were manipulated and treated as Unknown.

**Removed Attributes**

Attributes Caused\_by, Vendor, RFC, problem\_id, cmdb\_ci has been removed as there are 98% of data information is missing and we decided to remove the column if more than 78% of the data is missing in the database.

**Negative Values Attributes**

One of the attributes ‘Incident\_State’ which has negative value data including 8 levels of stages present in cells such as Active, Awaiting, closed, resolved, etc. the negative value has been replaced with reasonable state value.

### 3.1.1 Staging data mapping etl

The flat file ‘Incident\_Event\_log.csv’ data source was imported into the staging SQL Server database after replacing the missing value.

Text

Description automatically generatedDiagram

Description automatically generated

### 3.1.2 Data Warehouse ETL

The Data Warehouse dimension and fact table were created and loaded using the staging and the primary key for each dimension and fact table were identified and set using the feature of SSMS.

**Incident Dimension ETL**

Graphical user interface

Description automatically generated

**Category Dimension ETL**

Diagram

Description automatically generated

**Status Dimension ETL**

Diagram

Description automatically generated

**Date Dimension ETL**

Diagram

Description automatically generated

**Priority Dimension ETL**

Diagram

Description automatically generated

**Fact ETL**

Diagram

Description automatically generated

**Load Data Warehouse**

Graphical user interface

Description automatically generated with medium confidence

# 4. VISUALIZATIONS AND REPORTS

## 4.1. Visualizations

### Categories wise Incident

Chart

Description automatically generated

Categories are the departments that are responsible to handle the incidents based on their priority. Here we have generated the top 10 categories which are handling most of the incidents. By looking at the graph we can have a general understanding that each incident is scanned and placed in its respective categories based on their similarities. We have encountered over fifty categories while handling this project and generated the top 10 categories which are responsible for handling the most occurring incidents.

### Priority Incident Count

Chart, bar chart

Description automatically generated

As the name suggests, priority incidents are incidents divided into different groups based on how much they affect the business. Here we have divided these incidents into four different sets of priorities. Starting with Critical, which are the most important issues, followed by High priority, Moderate priority, and lastly Low priority incidents. Categorizing these incidents based on their priorities, the business will have a clear idea of how many resources they should spend on them and how much time would be consumed solving those incidents, thereby saving time and money.

### Total Reassignment

Chart, line chart

Description automatically generated

Whenever a category handling an incident fails to close the issue, that incident is re-assigned to a different category and it keeps getting reassigned as long and the incident remains. If we look at the graph, we can see that category 42 have an overall of 3757 incident cases out of which 15 incidents are re-assigned to hem from a different category that failed to close those incidents. Category 26 has an overall of 3,369 incidents out of which 18 incidents have been re-assigned to them from a different category. This type of data can help the business to maintain records of the incidents that need to be given higher priority or to be allotted to categories with people having better skills in handling such incidents.

### Average Closing time

Chart, histogram

Description automatically generated

Each incident reassigned is tracked in the system which stores its information. One of that information is the average time taken to close a particular incident. In this graph, we can see the reassigned incidents and their average closing time. For example, if we look at day one, we can see that 800 incidents were reassigned to a different category which took a total of 12.269 hours to close. Similarly, if we look at day 15, we can see that 900 incidents were re-assigned to a different category which took an overall of 13.19 hours to close. Such tracking of assignment, re-assignment, and a closing average of incidents can be helpful in future prediction of resources and time consumption of the business and help them in finding a better solution to counter such incidents.

### Dashboard

A picture containing chart

Description automatically generated

## 4.2. SSRS Reports / Visualization

### Yearly incident count

Chart, bar chart

Description automatically generated

The number of incidents reported in the year 2016 and 2017. This graphical data consists of all the different categories of incidents occurring throughout the year. The steep decline in the graph from 2016 to 2017 proves the importance of incident management and how having a proper managing system can help us solve redundancies and improve the overall working of the business.

### Yearly Detailed Report

Graphical user interface, table

Description automatically generated

The above reports represent the detailed summary of each year that can be obtained using SSRS reports. By clicking on each year an individual report is generated as shown above. This is a detailed report containing every small detail of the incident such as incident number, category, creation date, the impact of the incident on the company, priority of the incident, and closing date.

### Service Level Agreement(SLA)

Chart, pie chart

Description automatically generated

SLAs are an agreement between the client and the company which determines the threshold of tolerance allowed regarding issues generated while handling a project. Currently, the graph depicts that 63.42% of the incidents are resolved within the aggreged time and with rules defined by organizations properly while 36.58% of the incidents are crossing SLA. Suppose if the SLA tolerance is 50% then if the Violated graph exceeds this mark, the company legally falls under threat and the client can impose a penalty or take major actions against the company.

### Priority Overview and detailed

Chart

Description automatically generated

Incidents divided into different groups based on how much they affect the business. Here we have divided these incidents into four different sets of priorities. Starting with Critical, which are the most important issues, followed by High priority, Moderate priority, and lastly Low priority incidents. Categorizing these incidents based on their priorities, the business will have a clear idea of how many resources they should spend on them and how much time would be consumed solving those incidents, thereby saving time and money.

Table

Description automatically generated

Each priority can be obtained using SSRS reports. By clicking on each priority an individual report is generated as shown above. This is a detailed report containing every small detail of the incident such as incident number, category, creation date, the impact of the incident on the company, priority of the incident, and closing date.

See Appendix A for code

# 6. Conclusions

An Incident is considered as a bug/error/event when the issue has been reported in the Information technologies /financial services organizations which may result in failure of activities or an existing system and affect the complete business. Using Data warehouse implementation on top of the current system will reduce the future re-occurrence of similar kinds of bugs/hazards and reduce completion time, time-saving, and can make team more productive to manage such a reportative task. Using this solution we can also easily identify and track every incident and to manage SLA committed by an organization

# 7. Bibliography

Amaral, C. and Fantinato, M., 2021. *UCI Machine Learning Repository: Incident Management Process Enriched Event Log Data Set*. [online] Archive.ics.uci.edu. Available at: <https://archive.ics.uci.edu/ml/datasets/Incident+management+process+enriched+event+log> [Accessed 23 December 2020].

www.javatpoint.com. 2021. *ETL Architecture - Javatpoint*. [online] Available at: <https://www.javatpoint.com/etl-architecture> [Accessed 29 December 2020].

Guru99.com. 2021. *Star And Snowflake Schema In Data Warehouse With Examples*. [online] Available at: <https://www.guru99.com/star-snowflake-data-warehousing.html> [Accessed 6 January 2021].

Docs.microsoft.com. 2021. *Functions (SSIS Expression) - SQL Server Integration Services (SSIS)*. [online] Available at: <https://docs.microsoft.com/en-us/sql/integration-services/expressions/functions-ssis-expression?view=sql-server-ver15> [Accessed 2 January 2021].

Docs.microsoft.com. 2021. *Lesson 7: Add Drillthrough Action On Parent Report - SQL Server Reporting Services (SSRS)*. [online] Available at: <https://docs.microsoft.com/en-us/sql/reporting-services/lesson-7-add-drillthrough-action-on-parent-report?view=sql-server-ver15> [Accessed 15 January 2021].

Tableau. 2021. *Data Visualization Beginner's Guide: A Definition, Examples, And Learning Resources*. [online] Available at: <https://www.tableau.com/learn/articles/data-visualization#:~:text=Data%20visualization%20is%20the%20graphical,outliers%2C%20and%20patterns%20in%20data.> [Accessed 7 January 2021].

# Appendix A – VISUALIZATIONS Code

--Incident Priority Overview

select year,priority,count(incident\_number) as cnt from(

select distinct priority,incident\_number,year

from Fact\_Incident F

join Dim\_Incident I on f.Dim\_Incident\_Key=I.Dim\_Incident\_Key

join Dim\_Date d on f.Dim\_Date\_Key=d.Dim\_Date\_Key

join Dim\_Priority p on f.Dim\_Priority\_Key = p.Dim\_Priority\_Key

where year in(@Year)

)a

group by a.priority,a.year

--SLA Overview

select count(incident\_number) as Count,case when sla =0 then 'SLA Vialated' ELSE 'Within SLA' END AS SLA from(

select distinct incident\_number,SLA,year

from Fact\_Incident F

join Dim\_Incident I on f.Dim\_Incident\_Key=I.Dim\_Incident\_Key

join Dim\_Date d on f.Dim\_Date\_Key=d.Dim\_Date\_Key

join Dim\_Category c on f.Dim\_Category\_Key=c.Dim\_Category\_Key

join Dim\_Status s on f.Dim\_Status\_Key=s.Dim\_Status\_key

where year in (@Year) and s.Status\_Description='Closed'

)a group by a.sla

--Incident Summary

select distinct year,count(incident\_number) as Inc\_count from

(

select distinct year,incident\_number

from Fact\_Incident F

join Dim\_Incident I on f.Dim\_Incident\_Key=I.Dim\_Incident\_Key

join Dim\_Date d on f.Dim\_Date\_Key=d.Dim\_Date\_Key

join Dim\_Category c on f.Dim\_Category\_Key=c.Dim\_Category\_Key

where year in (@Year)

)A

group by A.Year

--priority Detailed

select distinct I.incident\_number,c.category,c.sub\_category, inc\_created\_date,impact,priority,customer\_number,inc\_closed\_Date

from Fact\_Incident F

join Dim\_Incident I on f.Dim\_Incident\_Key=I.Dim\_Incident\_Key

join Dim\_Date d on f.Dim\_Date\_Key=d.Dim\_Date\_Key

join Dim\_Category c on f.Dim\_Category\_Key=c.Dim\_Category\_Key

join Dim\_Priority p on f.Dim\_Priority\_Key = p.Dim\_Priority\_Key

join dim\_status s on f.dim\_status\_key=s.Dim\_status\_key

where year in(@year)

and priority in (@Priority)

--Incident detailed

select distinct I.incident\_number,c.category,c.sub\_category, inc\_created\_date,impact,priority,customer\_number,inc\_closed\_Date

from Fact\_Incident F

join Dim\_Incident I on f.Dim\_Incident\_Key=I.Dim\_Incident\_Key

join Dim\_Date d on f.Dim\_Date\_Key=d.Dim\_Date\_Key

join Dim\_Category c on f.Dim\_Category\_Key=c.Dim\_Category\_Key

join Dim\_Priority p on f.Dim\_Priority\_Key = p.Dim\_Priority\_Key

join dim\_status s on f.dim\_status\_key=s.Dim\_status\_key

where year in(@year)**rs.CustomerID;**