Tarcísio Talles Dias Pereira

Tailoring a data analysis methodology to the Information Technology Service Management

Turin (TO)
March / 2020

Tarcísio Talles Dias Pereira

Tailoring a data analysis methodology to Information Technology Service Management

A thesis in the field of Information Technology for the degree of Master of Science in Engineering and Management.

Supervisor:
Prof. Dott. Tania Cerquitelli

DEPARTMENT OF MANAGEMENT AND PRODUCTION ENGINEERING
POLITECNICO DI TORINO

Turin (TO)
March / 2020

Acknowledgments

Studying and working is not always an easy life to equilibrate, thus I need firstly to thanks my directly managers John, Barbara and William for their comprehension. Barbara was also very available and helpful with the development of this thesis, as it were John, Nick, Carlos, Federico and Archna representing their regions. A special mention to Carlos, Vania, Rogério, Luís and all the LATAM team that were awesome colleagues in the onboarding project to Drive IT.

Thanks also to my friendly colleagues of Drive IT support: Alberto and Morena. I will never forget also the support and trust deposited on me by all Solve team, specially Deb and Paolo, dear colleagues since FCA time. Thanks also for FCA Drive IT team, which I have been part during three years working for FCA in Brazil.

Finally, thanks to Professor Cerquitelli, who taught me Business Intelligence – and made me fall in love with data analysis – and accepted my thesis proposal.

" The Information Age offers much to mankind, and I would like to think that we will rise to the challenges it presents. But it is vital to remember that information — in the sense of raw data — is not knowledge, that knowledge is not wisdom, and that wisdom is not foresight. But information is the first essential step to all of these."

-- Arthur C. Clarke

Abstract

Information technology services are essential for any company that wants to keep competitive in the market. All business units and productions process are supported by computers, mobile devices, applications, etc. In this scenario, quality and working IT services becomes crucial for organizations. What if an IT service fail? A dedicated process in the Information Technology Service Management (ITSM) library deals with fails: Incident Management.

An incident is a failure or loss of quality perceived in a service. When an incident is noticed, the user – so called end user – needs to report the fault for responsible IT support teams to work on its resolution. In order to report the issue, the end user can have different channels available such as a telephone number to call or a self-service portal to register it. After an incident is reported, a proper support team (depending on some characteristics like nature of service and location of user) will be in charge of it. The incident can be also reassigned to other teams during the resolution process. When it is fixed, it should be properly closed.

All this process, from the incident logging to its closure, is normally registered and managed using an ITSM platform. There are diverse options in the market and CNHi and FCA decided to implement the ServiceNow platform together in a customized instance called Drive IT. However, there were many differences in CNHi and FCA processes that should be considered and addressed. The same was valid inside each company and its regions. The objective of this work was to use data analysis to identify, analyze and evaluate the Incident Management process implemented by the four regions (APAC, EMEA, LATAM and NAFTA) of CNHi in Drive IT.

Index

Pictures List

Tables List

Abbreviations and Acronyms List

IT	Information Technology
ITSM	Information Technology Service Management
HD	Help Desk
SD	Service Desk
EUS	End User Services
BI	Business Intelligence
SaaS	Software as a Service
SLA	Service Level Agreement
MTTR	Mean Time to Repair
ROI	Return on Investment
ITIL	Information Technology Infrastructure Library
COBIT	Control Objectives for Information and Related Technologies
MOF	Microsoft Operations Framework
CI	Configuration Item
OOTB	Out of the Box

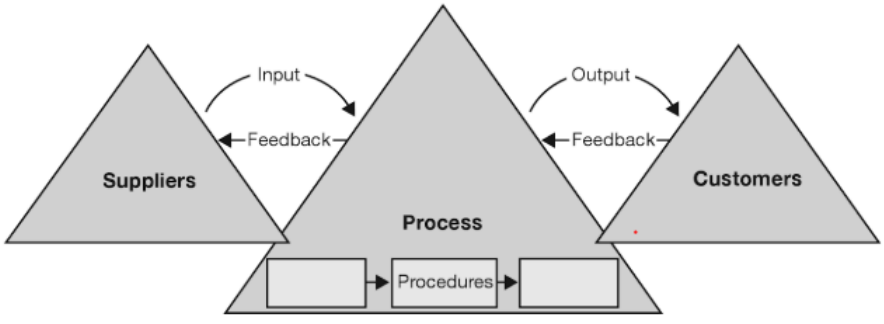
1 Introduction

The technology is present in our lives, in our daily activities, at home, university, work, everywhere. There is no business running in nowadays without information technology. From small and local business, to large and multinational companies, information technology is present in many activities, supporting production process, decisions makings – specially by the staff –, and any other area that uses a computer, a tablet, a smartphone and other technologies. The supply and use of these technologies require process and tools to manage it. In this scenario, it was born the concept of Information Technology Service Management (ITSM).

The first international standard for ITSM, ISO/IEC 2000, defines it as "an integrated process approach that enables an IT organization to deliver services that meet business and customer requirements". According (Knapp, 2010), the consistent use of a well-designed and implemented process of ITSM enables IT organizations to:

- Align their efforts with business goals
- Ensure compliance with applicable regulatory controls
- Achieve customer and employee satisfaction

The ITSM role in organizations is to define and manage the interactions between suppliers and customers through processes, like showed in the Figure 1 bellow:



Picture 1 - Process Model (Source: Knapp, A Guide to Service Desk Conceptions, 3E. 2010, South-Western)

The ITSM is responsible to manage the delivery of IT services, but it also uses technology in its processes and activities. For example. the Service Desk uses telephone to

receive calls from users that have needs, then they register that needs in a ticketing tool, where a support team manages the ticket. There are many ticketing tools in the IT market, and they had evolved a lot in the last years, including new technologies like reporting, notifications, artificial intelligence and others. Gartner, one of the most respectable IT consultant institutions in the world, used to classify technology elements (like tools and methodologies) in its famous magic quadrant, where these elements are distributed according their characteristics. On July 2019, Gartner released the last magic quadrant comparing the main tools for ITSM in the market:

Picture 2 - Magic Quadrant for ITSM Tools (Source: Gartner, 2019)

Looking to the chart, it's possible to see that there are two leaders: ServiceNow and BMC. While BMC is a little bit more visionary than ServiceNow, ServiceNow is considerably more executable than BMC. In 2013, Fiat Chrysler Automobiles (FCA) and CNH Industrial (CNHi), decided to unify the ITSM processes and tools among the companies and regions in all the world. At that time, each company and region were using its own processes and tools

and standardize them was a very important step to enable a global management and continuous improvement in ITSM in the group. It was decided to adopt the ServiceNow as the official and global ITSM tool for all companies and regions. One of the reasons of this decision was that ServiceNow was already considered leader in ITSM by Gartner (even more at that time, being both the most visionary and most executable), as that is showed by the magic quadrant released in 2014:

Picture 3 - Magic Quadrant for ITSM Tools (Source: Gartner, 2014)

The tool was chosen, and main go-live was done in 2015, but each company and region had the autonomy to decide and plan when to on board to ServiceNow, that the customized instance for the project was named Drive IT. With a single tool and standard processes, Drive IT brought also a unified data structure for ITSM in the company.

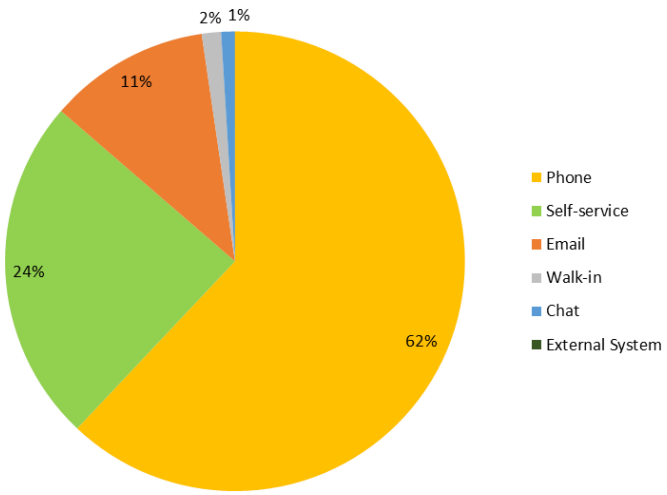
To keep competitiveness in the current Market, any company must invest in processes improvements. Improving processes can result in lower costs, higher profits, higher quality and many other benefits. To improve processes, companies must manage data. This duality between data and processes always existed and it shows that these two pillars are critical in companies that intent to have reputation, via quality (Barbieri, 2012). The focus of this work

is to propose a methodology that enable improvements in ITSM process of CNHi, using data as the main resource.

1.1 *Motivation*

With new technologies available, new possibilities and opportunities raise, especially for improvements. As already mentioned before, the traditional ITSM structure has a Service Desk (SD) which receives calls from users and register them in a ticketing tool, assigning each ticket to a support group according some characteristics like affected service or item, user location, etc. Usually, the SD has scripts with simple instructions to try to resolve simple cases or to collect required information from the caller and follow those instructions to register and assign the ticket. Keeping a Service Desk team has a cost. Some contracts are invoiced by the number of calls/interactions the analysts receive, other contracts are made with fixed price, defining a maximum number of hours to use or minimum personnel available in a period, among others.

ServiceNow introduced the possibility to automatize the process of routing tickets, based on information provided by the user (or already present in the system). The user can, for example, access a website and report an issue or request a service, instead of calling to the Service Desk. In the past, to operate IT systems, it was required some minimum skills that most people may didn't have. Nowadays, it's hard to find someone that doesn't have a smartphone or a computer and is not able to use a website. However, even so, many people are still contacting the Service Desk for IT needs, as showed by the chart below:



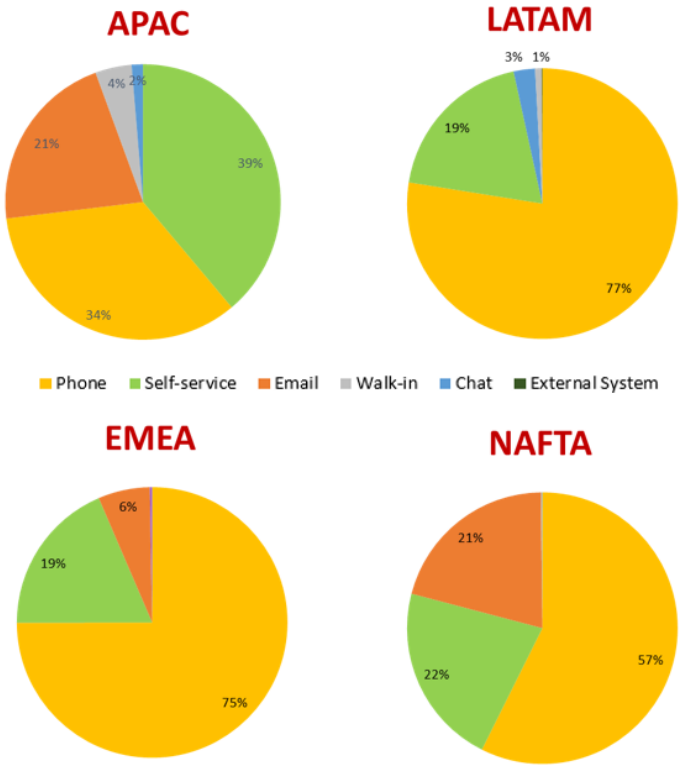
Picture 4 – EUS incidents by Contact Type (Source: Drive IT, October 2019)

This data was extracted from Drive IT considering all the incidents closed by EUS (End User Services) groups from CNHi in Drive IT in October 2019. Looking to the chart, it's easy to perceive that calling to the Service Desk is still the most preferred channel for users. Considering the more user-friendly IT systems and that workers are higher skilled in IT nowadays, one of the objectives of this work was to investigate why users are still using Service Desk that much.

CNHi is divided in four regions and, even if Drive IT has unified the ITSM in the company, each region one has its differences in processes, tools and culture. The regions are:

- APAC: Asia and Pacific
- EMEA: Europe, Middle East and Africa
- LATAM: Latin America
- NAFTA: North America

In order to propose improvements in the ITSM process, it's important to understand each region's specificities. For example, doing a drill down by region in the data collected, it's possible to see that in some regions, the Service Desk is even more used than in others (see Picture 5 below). On the other hand, there are some regions using more the Self-Service and it could be investigated why.



Picture 5 - EUS incidents by region and contact type (Source: Drive IT, October 2019)

It's possible to drill down the analysis by many other characteristics of the incident and each information can be used as input for an improvement or decision making. Or even a collection of information can be analyzed together to produce other derivative information as output. Thus, this work proposes a methodology to collect, analyze and use this information with the aim to improve the management of IT services within CNH Industrial.

1.2 *Objectives*

The first and main objective of this work was to provide the company a methodology to collect, analyze and use data from incident management activities registered in Drive IT with the purpose of improving the IT services and its management through all the regions of CNH Industrial. Improving the ITSM processes, company may save money, for example reducing (or even eliminating) the costs with a service that may is not necessary. If users create the tickets by themselves directly in the portal, contacting the Service Desk would be necessary only in exceptional cases (e.g. when system is down, or user can't log in). If the contract with the Service Desk is invoiced by number of interactions, the count is simple: less interactions, less costs. If it's based in a fixed number of hours or minimum personnel available, the low demand can lead to a renegotiation or a lower new contract in the future.

Improvements in the processes could also bring more advantages than only costs saving. Other objectives of this work are:

- Improve data quality on ticket creation: each time user calls to the Service Desk, he needs to inform some personal data like user ID, department, location, etc. Using the portal, for example, this information can be automatically taken from user's profile. As a side effect, it would be improved also the correctness and completeness of data.
- Improve data quality on ticket closure: an incident is classified according its cause and resolution provided by the technician assigned to it. This data is very important to provide information for the methodology of data analysis. The methodology itself can provide improvement opportunities to better classify tickets and standardize classifications among the regions.
- Reduce the number of tickets created: knowing common causes and solutions for incidents, it's possible to identify cases where a simple instruction could be

enough, without engaging the technical team. Instead of being given by a man, these instructions can be given by the system via knowledge base or by a smart agent trained with artificial intelligence.

- Reduce the fulfilment time for IT services: sometimes the incidents are assigned to incorrect groups by the SD analyst and they remain open for a period before being reassigned or cancelled. Using the feature of routing rules, it's possible to automatically route incidents to the correct resolver groups, based on information like user's location, service desired, etc.
- Provide valuable and useful data for stakeholders: going from generic and manual input data to automatized and detailed information can be very helpful for stakeholders (e.g. managers) to evaluate and improve their processes. Information can provide valuable inputs for decision makings.

1.3 *Text Organization*

This text is organized to start introducing the current scenario of the use of data analysis in ITSM, giving a high-level picture of related works (academic and corporate). An investigation was done to find important projects and initiatives related to the main subject of this work. After introducing the related works, fundamental concepts to understand this work are presented. These concepts are widely used in IT environments but may be new for non-IT people. The main knowledge needed to follow this work is to understand the ITSM world and the incident process. In addition, also some concepts of data analysis like business intelligence are introduced.

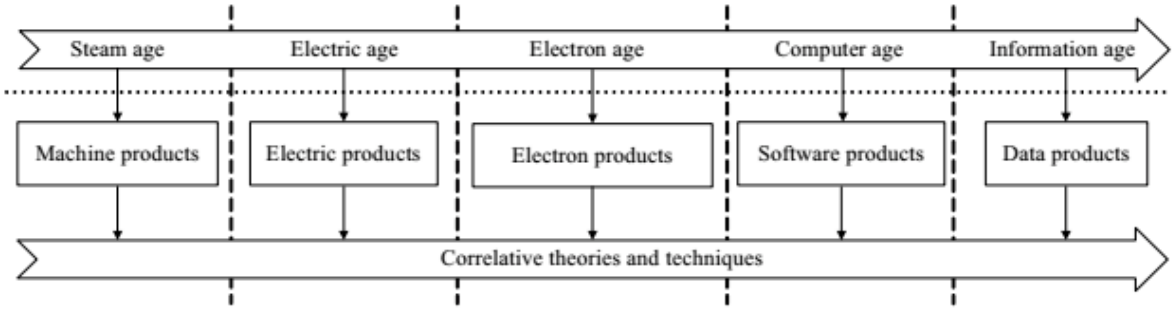
After presenting the essential concepts to understand the work and the current state of data analysis applied to ITSM, the methodology of the work is explained and then the core part is explored: the analysis of incident data collected in CNHi during four months for the four regions. Finally, conclusions, the work's contributions and possible future works are listed.

2 Related Work

Data analysis and ITSM are not very new concepts, but even so, there are not many academic works relating both. From the researches done in Google Scholar, very few results were obtained about data analysis applied to ITSM (and some variances in the verbiage). Maybe the reason is because the ITSM tools had improved a lot in the past few years, providing better data and enabling trustable and useful data analysis. Before, the ITSM processes were very dependent of human actions, supported by simple ticketing tools with limited data and reporting features.

Many results returned from the researches are about ITSM, IT services, data analysis, data governance and other related concepts. Basically, the field of information technology services and the subject data were very explored by the community in the past years. Information Technology Service Management has become a popular research area as a result of industry push and the development and advancement of research in service sciences (Shahsavarani & Ji, 2011). The focus on services has been growing in the last years due to the development of IT industry that offer many opportunities for organizations to manage IT and information resources based on service model. As a result, organizations, business or otherwise, in the world are shifting from a goods-based economy to a service-based economy (Rai & Sambamurthy, 2006).

IT services are, normally, services involving resources (e.g. people), processes and technological items like a platform. A good example of service that became very popular in the past years is the Software as a Service (SaaS), which substitute the traditional model of having a software locally installed in personal computers. These IT services can be considered part of software products of the Computer age, as proposed by (Cao et al., 2010). Second their studies, the technology evolution and its products can be divided in five different ages, as shown in the Picture 6.



Picture 6 - The evolution of the product (Source: Cao et al., 2010)

The products of all these ages are still present in our lives, some more, some less, and they are complementary between them. This is especially valid for the Computer and Information Age. Data are the new products, but they are not actually produced only from the Information age. Data were already produced before, mainly by software products, but they had been seen exclusively as computational asset, and not a unique valuable product. Now, in the age where information became spread as never before and it is fundamental for any company, data is seeing as organizational asset, with a high value for the business.

Although the valorization of data as an organizational asset, its use to support business in decision makings is not something that new. Second Primark (2008), the term Business Intelligence, or simply BI, was firstly mentioned by Gartner Group, in the 80s, and it was related to the smart process of collecting, organizing, analyzing, sharing and monitoring data, generating information to support decision makings in the business units.

Relating ITSM and data analysis, there are many articles written by IT professionals in sites and blogs like LinkedIn. In one of them, Iyengar (2016), explains how analytics can improve the IT service management in organizations and make happier the end user. He defines five key points where the analytics can impact the ITSM within the companies:

- **Minimize Impact of Business Downtime**: calculating metrics like MTTR (Mean Time to Repair), anticipating outage services and improving communication with users.
- **Optimize Resource Management:** monitoring the balance between tickets (demand) and resources (like technicians and Service Desk). Knowing the company needs, it's possible to optimize the allocation and use of resources.
- **Improve Service Quality:** comparing resolution (e.g. time) and re-opening rates, for example, to evaluate the efficiency of the work being delivered.
- **Maximize ROI on Software Purchases:** controlling the license usage and evaluating the real utilization to identify unnecessary licenses and reduce costs.

- **Ensure High Levels of End-user Satisfaction:** automating tickets assignment based on routing rules and track tickets resolution with SLAs (Service Level Agreement).

3 Essential Concepts

In order to understand this work, it's necessary to define some fundamental concepts that will be present through its development. Two of the most basic of them are data and information. For (Hoffer et al., 2007), data is defined as "stored representations of objects and events that have meaning and importance in the user environment", while information means "data that were processed in order to increase the knowledge of the person using them". From information, comes the knowledge that, for (Drucker, 2003), can be defined as "information that changes something or someone, becoming reason for actions, or making an individual (or institution) capable to act in a different or more efficiency way".

Another basic concept to understand that is essential for this work is what is a service and its differences from a good. While goods are physical objects, services are activities performed by a person or company to a third part. The Table 1 shows the basic differences between goods and services, helping to understand better the concept of this last one.

Table 1 - Differences between goods and services. (Source: Surbhi, 2018)

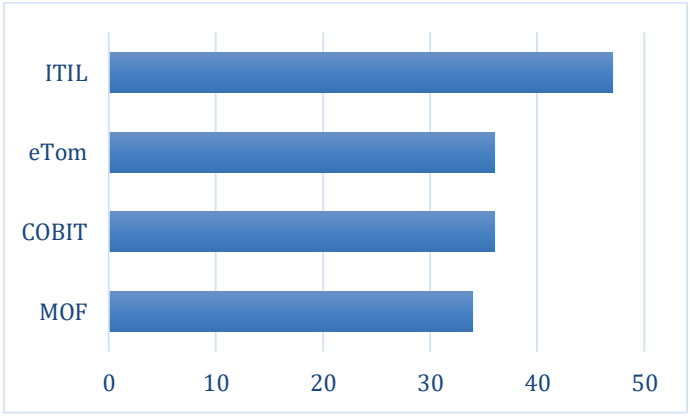
BASIS FOR COMPARISON	GOODS	SERVICES
Meaning	Goods are the material items that can be seen, touched or felt and are ready for sale to the customers.	Services are amenities, facilities, benefits or help provided by other people.
Nature	Tangible	Intangible
Transfer of ownership	Yes	No
Evaluation	Very simple and easy	Complicated
Return	Goods can be returned.	Services cannot be returned back once they are provided.
Separable	Yes, goods can be separated from the seller.	No, services cannot be separated from the service provider.
Variability	Identical	Diversified
Storage	Goods can be stored for use in future or multiple use.	Services cannot be stored.
Production and Consumption	There is a time lag between production and consumption of goods.	Production and Consumption of services occurs simultaneously.

Summarizing, services are the intangible economic product that is provided by a person or company on the other person's or company's demand. It is an activity carried out for someone else. From this concept it's easy to understand what information technology services is: services provided in the technology field. These services are demanded by most of companies today, specially the big ones, because they have automated processes for production, distributing, accounting and many other business and administrative units. Besides the organizational infrastructure and diverse applications used, employees need equipment like computer, smartphone, etc. To manage the processes, resources and services involved in information technology demands in a company, it was arising the concept of Information Technology Service Management (ITSM).

3.1 *Information Technology Service Management*

Information Technology Service Management, or just ITSM, is a subfield of Service Science that focuses on defining, managing, delivering, and supporting IT services to achieve organizational goals (Shahsavarani & Ji, 2011). It provides benefits for organizations by helping them become more adaptive, flexible, cost effective, and service oriented (Conger et al, 2008; Winniford et al., 2009). Interest in ITSM has surged because of the growing complexity of IT and the increasing maturity of IT management (Conger et al., 2008). Adopting ITSM, companies can align the IT operations with business goals.

There are different frameworks of ITSM that support organizations to implement and manage IT services. In 2017 The 2017, Forbes did a survey to evaluate the state of information technology service management. It surveyed 261 senior-level executives from around the world, representing organizations at various revenue levels from small (less than $500 million) to large (greater than $5 billion). Its survey results are shown in the chart below:



Picture 7 - ITSM Frameworks applied by companies (Source: Forbes Insight Survey, 2017)

These numbers are about the percentage of the interviewed executive that answered that his or her company applies a specific ITSM framework. A company may use more than one framework to design and implement its own ITSM process, thus, these numbers don't sum 100%. Even other frameworks were mentioned, but these were the most popular four.

Each framework has its own characteristics and specificities that are evaluated by companies according its business and purposes. COBIT (Control Objectives for Information and Related Technologies), one of the most popular frameworks, started in the financial audit community, but has since expanded to include management standards. On the other hand, eTom is commonly used by telecom services providers and MOF (Microsoft Operations Framework) is focused on managing the IT lifecycle (Hertvik, 2017).

Other framework with focus in IT lifecycle is ITIL, the most used one. ITIL means Information Technology Infrastructure Library and one of its main goal is to align IT services with business needs. CNH Industrial applies ITIL best practices to manage its IT services, thus this work followed the same framework.

3.2 *ITIL Framework*

The ITIL framework was introduced in the 1980s by the United Kingdom's Central Computer and Telecommunications Agency (CCTA). Currently it's owned, managed, updated, and certified by AXELOS (Hertvik, 2017). The framework defines best practices to manage IT services, like concepts, procedures, standards, etc. One of the concepts defines by ITIL is the IT service lifecycle.

Picture 8 - IT service lifecycle defined by ITIL (Source: Flycast Partners, 2018)

When defining an IT service, it's important to coordinate and control all the processes, systems, and functions needed to determine, design, deliver and support it. The focus should be on continual improvement of both the services and the process. The life cycle proposed by ITIL is organized in 5 stages consisting of 26 processes offering best practice guidance on implementing IT Service Management (ITSM). Each stage contains a set of processes, key principles, and activities relative to that area of ITSM (Flycast Partners, 2018).

As it can be seen from the lifecycle, there are not defined start or end point. Then, where to start designing an IT service? That's one of the biggest benefits of the IT service lifecycle proposed by ITIL: you can start at any point. The lifecycle is defined to be easy do adopt and adapt, according the business needs. It's possible to start from the strategy, driven by the staff, and design the service to meet business needs, but if there is already a service in operation, it's possible to adopt ITIL to manage it. The most important thing is to be always focused on continuous improvement of the IT services and processes.

In CNHi, there are IT services in all the stages of the ITIL lifecycle. But most of them are mainly in the operation stage, even if there are some initiatives to design new processes and features. This is how continuous improvement works: services in operations being improved and being used as input for processes improvements. The scope of this work is the EUS services – specifically the incident process – that is almost all in operation stage. The operation stage has the following objectives:

- Deliver services to authorized users
- Deliver services within service levels
- Optimize cost and quality
- Execute operational controls
- Build and maintain user satisfaction
- Minimize service outage impact
- Enable business outcomes

In order to achieve its objectives, each stage defines processes to support with activities, procedures, functions and all the other elements needed to fulfill a stage. In the case of operation stage, the processes defined are:

- Incident Management
- Request Fulfillment
- Event Management
- Problem Management

- Access Management

It defines also some functions that are essential in this stage like Service Desk, application and technology support and facilities management. Delimiting even more the scope of this work, the methodology using data analysis will be proposed for the Incident Management process.

3.3 *Incident Management*

Before introducing the incident management process, it's essential to define the concept of incident. As defined by the ITIL framework, an incident is an unplanned interruption or a reduction in the quality of a service, or a failure of a configuration item that has not yet impacted a service.

The main purpose of the incident management process is to restore the service to its normal operation as soon as possible and minimize the negative impact to the business. The process of incident management is responsible to manage an incident through its entire lifecycle, from when user reported the fault until its solution be provided. An incident can be resolved with a temporary workaround or a definitive solution. Other objectives of the incident management process are:

- Ensure that methods and procedures are used to prompt answer, analysis, documentation, continuous management and incident reporting;
- Increase the visibility and communication of incidents to the business and TI team;
- Improve and keep the business satisfaction regarding the TI through a professional approach, quickly resolving and communicating incidents when they occur;
- Align the incident management activities and their priorities with the business priorities;

To achieve these objectives, activities are defined within the process, from the ticket registration to its closure. The incident management activities defined by the ITIL framework are:

1. Incident identification
2. Incident registration
3. Incident categorization

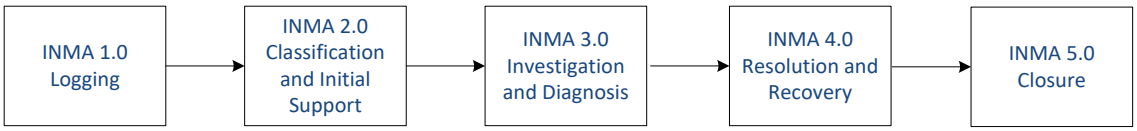
4. Incident prioritization
5. Initial diagnosis
6. Incident escalation
7. Investigation and diagnosis
8. Resolution and recovering
9. Incident Closure

The ITIL framework defines best practices, but, as the IT service lifecycle, the activities inside a process can be adopted and adapted. It's easy to find many different versions of incident lifecycle based on the ITIL standard, but modified. The picture 9 is an example:

Picture 9 - An adapted incident lifecycle (Source: ManageEngine, 2019)

4 *The Incident Management process in CNHi*

In CNHi and FCA, the ITSM processes were redesigned globally as the core of Drive IT Global Services project, to unify processes and tools. ITIL best practices were the basis to be followed, adapting it to organizational specificities and business needs. The definition of the incident lifecycle is the start point for the incident management process. Drive IT defined it simpler and shorter than the original one from ITIL as it can be seen in the picture 10 below.



Picture 10 - Incident Management Lifecycle defined by Drive IT project (Source: Drive IT Global Services, Incident management Process Guide, 2015)

Before explaining each one of the defined stages of the Incident Management lifecycle, it's necessary to introduce the concept of the roles and responsibilities and who are they in the Incident Management process defined by CNHi and FCA.

4.1 *Roles and responsibilities*

Roles and Responsibilities must be clearly defined to avoid multiple people being responsible for the same thing or the issue of nobody being responsible for the needed activities. Regardless the roles defined, the most important is to have all the activities of the process covered by someone. The table below details all the roles and responsibilities defined by Drive IT project for the Incident Management process in CNHi and FCA:

Table 2 - Roles and responsibilities for Incident Management Process (Source: Drive IT Global Services, Incident management Process Guide, 2015)

Role	**Description**	**Responsibilities**
Global Process Representative	Ability and authority to ensure the process is rolled out and used by the entire IT organization. Generally, a Senior Manager or Director.	• Accountable for the overall quality of the process and oversees the management of and compliance with the processes, procedures, data models, policies and technologies used with the IT business process. • Responsible for ensuring that the process is fit for purpose and for ensuring that all activities within the process are performed. • Responsible for the sponsorship, overall mission, design, and Change Management of the process and its metrics. • Communicating the process mission, goals and objectives to all stakeholders • Resolving any cross-functional (departmental) issues • Reporting on the effectiveness of the process to senior management • Initiates process review and any improvement activities
Incident Process Manager	This role may be fulfilled by multiple people or can be the same	• Reporting on Incident Management process activities

	Global Process Representative, depending the size and/or geographical locations of the ICT organization. This role supports the Global Process Representative with the effective rollout and execution of the process within the designated regional or organizational scope of responsibility. Generally Senior Managers.	• Review Key Performance Indicators and trigger improvement activities • Continuous Process Improvement • Definition of process rules and policies aligned with overall rules and policies • Provide tool support for the process • Ensure data quality • Implementation and utilization of reports showing lead indicators for imminent incidents • Verifying process execution and tools with process documentation • Solicit and track user feedback, client satisfaction, dashboards and metrics to measure success and engagement of new and existing process functionalities • Work with the Global Process Representative to review and prioritize improvements • Training of personnel
Incident Manager	This role may be fulfilled by multiple people depending the size and/or geographical locations of the ICT organization. This role ensures the effective operational	• Reporting on specific process activities • Continuous Process Improvement • Hierarchical escalation • Ensure data quality

	execution of the process. Generally Senior Managers.	• Implementation and utilization of reports showing lead indicators for imminent incidents • Manage resources assigned to the process • Work with service owners and other process managers to ensure the smooth running of services • Coordinating interfaces between incident management and other service management processes
Incident Owner	This is typically the service desk agent or the technical support staff who the incident is assigned to or the assigned resource responsible for tracking the whole end-to-end Incident lifecycle, ensuring that the issue will be solved	• Owning the Incident lifecycle • Recording the Incident • Monitoring and Tracking the status and progress towards resolution of owned Incidents • Communication about Incidents to appropriate stakeholders • Providing resolutions, quick fixes and workarounds from existing known error databases • Closing of incidents • Escalating Incidents as necessary per established escalation rules. • Validating Incident records have documented all relevant actions taken, information and

		that correct categorization has been applied prior to closure • Managing Major Incidents
Incident Coordinator	This role is the "point person" within a Support Group that is accountable for all Incidents assigned to their group.	• Is responsible for monitoring their respective queues for assigned Incidents and assigning them to the appropriate individuals within the Support Group for further investigation. • Also responsible for the speediness of solving the Incidents so that Resolution Targets are met. • Ensure data quality • Assigning Incidents to appropriate support groups • Monitoring the status and progress towards resolution of assigned incidents • Assigning Incidents to appropriate Support/Resolver groups (reroute when incorrectly assigned)
Incident Analyst	This is typically a (technical) support group analyst or subject matter expert (Level 2 and Level 3) and could be internal as well as external (vendor).	• Recording incidents • Analyzing for correct prioritization, classification and providing initial support • Keeping users and the Incident Owner informed about Incident progress

		• Escalating Incidents as necessary per established escalation rules • Performing additional investigation and diagnosis of assigned Incidents when required • Providing resolution and recovery of incidents • Updating Incident records with all relevant actions taken, information and ensure correct categorization prior closure • Assigned incidents back to the Incident Owner for confirmation and closure
Incident Submitter (Caller)	This is typically the user or technical support staff, or in case of automation, the monitoring or alerting applications.	• Reports an Incident or submits the Incident record • Participate in applying or implementing the quick fix, work-around or resolution • Confirm resolution of the Incident
Business Relationship Manager	This role is responsible for managing the relationship with the business for a particular set of services and/or business function/processes.	• Eventually participates of Major Incident, being part of the technical bridges, opening management bridges depending on the affected business and the impact of the issue and helping the communication activities

The platform chosen by Drive IT to manage IT services in CNHi and FCA was ServiceNow and it is based on the ITIL framework. ServiceNow is very customizable, however, from the out of the box (OOTB) solution, there are some definitions, like workflows and roles. These roles are described in the table below:

Table 3 – Incident process roles on ServiceNow

ServiceNow Role	Description
Created by	This is always who is logging the incident. This field is automatically filled in with the user logged while creating the ticket and can't be changed. He can be the Service Desk Analyst, the technical staff, the user himself or an external system, for example. Unless the created by is also performing other roles, this user will have no further activities in the incident.
Opened by	The opened by is generally the same of the created by, but not always. For example, an ICT user, may call the Service Desk to open a ticket on behalf of a business user. In this case, the Created by would be the SD analyst and the Opened by the ICT user reporting the failure. The Opened by can be just the Submitter, but he can be also the Incident Owner.
Affected User	The Affected User is generally the same of the Opened by – when he calls the Service Desk or report the failure from the Self-Service Portal himself – but someone can always call the Service Desk to report a ticket on behalf of another user. In any case, the Affected User will be the focal point for communications, tests and resolution

	confirmation. He can also reopen an incident if he realizes it's not resolved.
Assigned to	This is the technical for whom the incident is assigned for resolution. He can be the Incident Analyst (from L2 or L3 for example) or even the Incident Owner (e.g. the Service Desk Analyst or the technical staff). An incident can also be reassigned and involve more than one Assigned to, but only in sequential activities (one per turn).

The roles Business Relationship Manager (BRM) and Incident Coordinator are normally present in ServiceNow as the configuration item (application or service) manager and the resolver group manager, respectively. The BRM can also be defined regionally, but only one global responsible can be configured by configuration item. In some cases, the Incident Coordinator can be a high-level manager from the supplier that is not configured as managers of the groups he is responsible, because each group has specific lower level manager.

The roles of Global Process Representative, Incident Process Manager and Incident Manager are not present in ServiceNow as fields or user type. The first two, are very high-level generally performed by Senior Managers (in most cases the same person) and they are generally involved only in process reviews and benchmarks. They are not involved in single incidents and day by day activities of the process. The last one, Incident Manager, is generally someone internal from the ICT department that has a good know-how about the process and is responsible to manage its execution and track incidents resolutions. In order to support the Incident Manager to perform his role, he is member of the Incident Managers group, where he has some special access granted to visualize and modify any incidents, even those not assigned to resolver groups he is member or manager.

4.2 *The states of an incident on ServiceNow*

Like for roles, ServiceNow platform has an OOTB workflow. Drive IT decided to keep its processes as closer as possible to the OOTB solution of ServiceNow and following this, the

mapping between the incident lifecycle adopted by CNHi and FCA (showed by Picture 10) and the incident workflow defined by ServiceNow can be considered as:

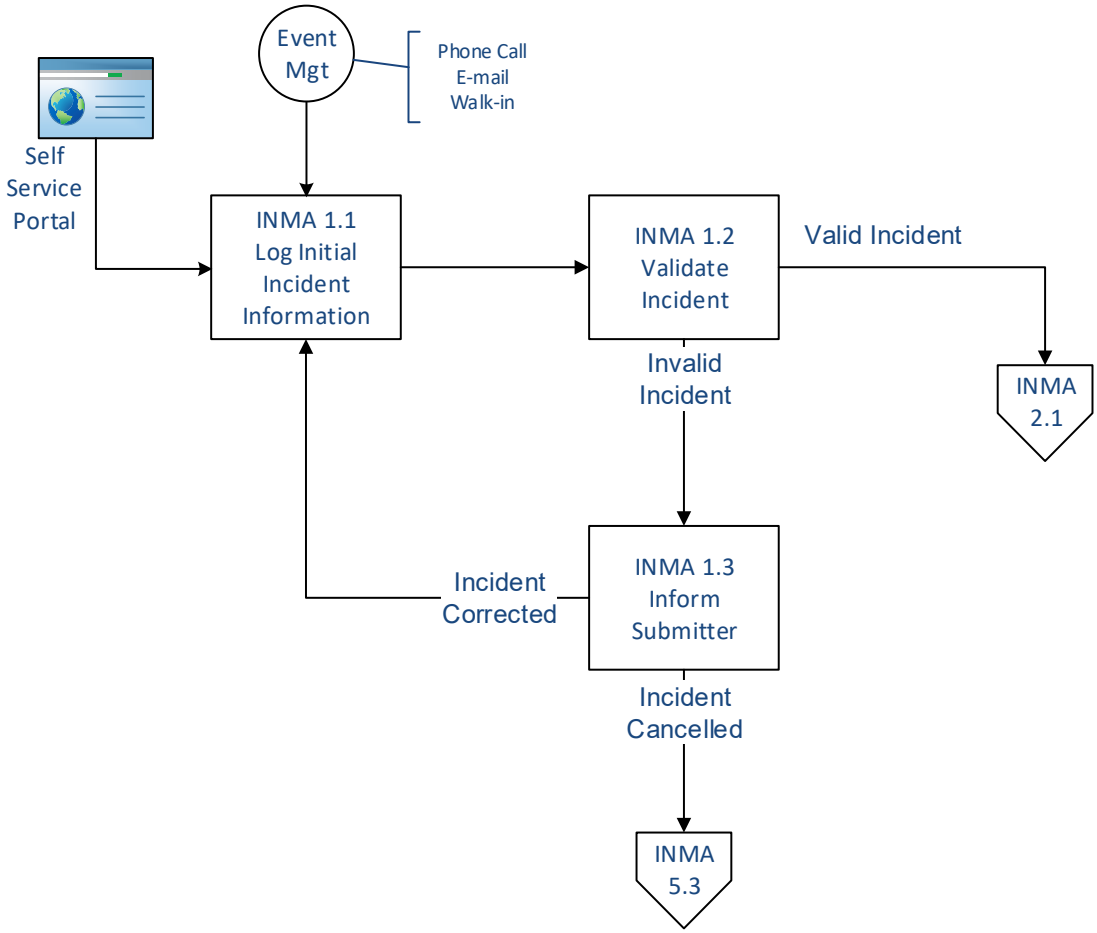
Table 4 - The OOTB states of an incident on ServiceNow

New	By default, it's the default value upon record creation. But as Drive IT is configured, all incidents are always assigned to a group, since its creation. Thus, the initial state of the incident is Assigned.
Assigned	That's actually the initial state of all incidents in Drive IT (the CNHi and FCA instance of ServiceNow), because all tickets are assigned according routing rules. In this state, ticket is assigned to a resolver group (set in the Assignment Group), but not yet to a specific technician (member of that group). In this state, any fulfiller user (with ITIL role) can update the ticket, even if he is not member of the Assignment Group. This state is equivalent to the stages Logging and Classification and Initial Support of the Incident Management Lifecycle.
Working in Progress	This is the state when someone in the assigned resolver group started to work in the ticket. This person will be set as the Assigned to and he/her is responsible to do the Investigation and Diagnosis of the incident. The state update to Working in Progress (WIP) is not automatically when the field Assigned To is filled in, but if the state is updated to WIP, it's mandatory to fill in the Assigned to. In this state, the ticket can be updated only by the Assigned to, any member of the Assignment Group and users with the role Incident Manager. In some cases, the technician assigned to the ticket needs more information or additional support, then he can put the ticket in pending state.
Pending	When the ticket is put on Pending state, eventual SLAs configured generally pause. A ticket in Pending can be considered part of the stages Classification and Initial Support or Investigation and Diagnosis in the Incident Management lifecycle. When putting a ticket in Pending, the technician is required to specify the pending reason:

	• **User**: it's necessary more information from the Incident Submitter (or even the Incident Owner). A work note detailing which information is missing is required and user is automatically notified. • **Supplier**: Incident Analyst is waiting for an answer from a third-party supplier who does not uses or integrates with the FCA/CNHI tool. If the supplier uses Drive IT, the correct procedure would be to reassign the incident to its adequate resolver group. • **Change**: some activity for recovering the service needs to be done by a change, which will happen in a window in the future. An associated change must be created and follow the Change Management process.
Resolved	The incident has been resolved but not yet confirmed with the customer or user. This state is equivalent to Resolution and Recovery in the Incident Management lifecycle and the analyst must provide required information about the resolution and cause of the fault. When the ticket is in this state, the Affected User, any member of the Assignment Group or an Incident Manager can reopen it at any moment, providing a reason why the incident is being reopened.
Closed	User satisfaction has been confirmed by the Incident Analyst or Owner and incident is manually closed, or the period for automatic closure is finished without the user reopen the ticket. The record can no longer be updated.

Now, knowing the roles and responsibilities and the Incident Management lifecycle of CNHi and FCA and its equivalencies on their ServiceNow instance, details of each stage of the lifecycle are introduced.

4.3 *Logging*



Picture 11 - Process of logging incidents (Source: Drive IT Global Services, Incident management Process Guide, 2015)

All Incidents must be fully logged and date-time stamped, regardless of the entry point (Self-Service, Service Desk, and Technical Support, via a telephone call, by email, chatbot, automatically detected or portal). All relevant information relating to the nature of the Incident must be logged so that a full historical record about the Incident is maintained – and so that if the incident has to be referred to other support group(s), they will have all relevant information on hand to assist them in the investigation and diagnosis. The entry points (as known as Contact Type in ServiceNow) for logging incidents defined by Drive IT Global Services and available using ServiceNow are:

Table 5 - Contact Types to report incidents on ServiceNow

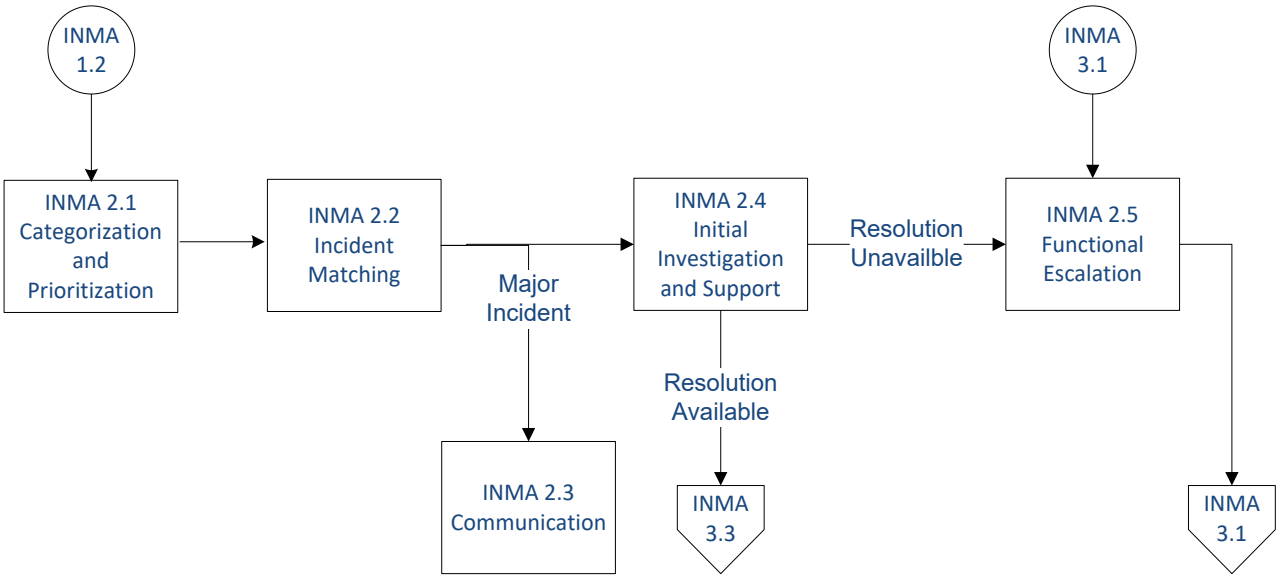
Self-Service	Any user with an account in IAM (the system to manager users' information in CNHi and FCA) is, by default, a Requester in Drive IT and can access the Self-Service Portal available to report fails in applications, services or hardware. The user information is automatically filled in for Opened by and Affected user, but they can be modified to any other active user in IAM. User is required to inform which application, hardware or service is failing (selecting a configuration item) and describe the issue with free text. Then, user needs to answer some questions to evaluate the impact of the issue and the urgency of having it resolved. These two information combined defines the incident priority, but from the portal it's not possible to create major incidents (maximum priority from there is P2).
Phone	An end user facing an issue with any IT service or equipment can call to the Service Desk to report it. Each region (or country) has its own Service Desk, providing support in local language and local business time. The availability of the service, its capacity, calendar and schedule are defined according local and services' needs. When a SD Analyst receives a call to register an incident, he used to follow a script or template (can be defined in ServiceNow). Firstly, the call must be registered, classified as incident and a short description provided. The contact type must not be changed and kept as Phone. When it's submitted, an incident is automatically created with same Opened by (generally the SD Analyst), Affected User (generally the caller) and call's short description. The analyst must, then, fill in the missing mandatory information to complete the incident registration (affected service or application, configuration item, assignment group and description). The assignment group can

	be automatically filled by routing rules after the configuration item selection. The analyst should confirm if it's correct, as well the priority. In cases when the SD analyst can resolve the issue himself during the telephone call, the ticket call created must be classified as first call resolution and the ticket incident should not be created.
Email	Another contact channel present in some regions for the Service Desk is the e-mail. In regions where it's available, when an email is received by the address configured by the local Service Desk, it's automatically converted in a ticket call in Drive IT (with contact type as Email), a SD Analyst takes it and the process that follows is the same when a telephone call is received. This channel is available in APAC, EMEA and NAFTA. Only LATAM didn't active the e-mail channel for Service Desk.
Chat	Similar to Phone and Email, when users have contact directly with SD analysts via chat (e.g. Skype) and report an issue. For a long time this was not an official and very used channel, and there were no definition in the process if the analyst should create the call as the first step or if he could create only the incident. Recently, LATAM implemented the possibility of contacting the Service Desk via WhatsApp and defined the process to follow similar to the one for telephone calls, but classifying the contact type as chat.
Walk-in	When an end user goes directly to a technical staff or a fleet analyst, for example, to report an issue, it should be registered as an incident with Contact Type Walk-in. Normally, SD agents will not be contacted by walk-in, because the Service Desk usually is isolated from the working sites. This type of contact tends to grow in CNHi, because recently it was released the Walk-up experience feature by ServiceNow to support the Tech Stops on sites. The Tec Stops are strategic places within the working sites where the fleet teams or any

	other technical staff are available to give support by order of arrival or previous appointment.
External System	External systems can create incidents in ServiceNow using API (Application Programming Interface). ServiceNow provides native plug-ins, but Drive IT has defined its own API that is the only way to integrate external systems to Drive IT. Currently Drive IT API allows only the creation of incidents, but it is in its roadmap to include the possibility to consult incidents also. One example of the use of API to create incidents in Drive IT is the monitoring systems running in specific applications that automatically create tickets when identified anomalies. These tickets normally have as configuration item the application being monitored and as Created by, Opened by and Affected user the generic user created for the monitoring system. Another example are external interfaces that create tickets only upon user request.
Virtual Agent	Virtual Agent is one of the best examples of External System that creates incident upon user request. Using chatbots that can talk with users as it were a Service Desk agent. These chatbots can be trained using artificial intelligence to continuous learn and increase their capacity to resolve an issue without the need to create an incident and engage a support team. In the beginning of the analysis, no region was using virtual agents, but during the development of the work, LATAM released a solution integrating Skype for Business and Drive IT. This solution from the provider Stefanini allowed users to create incidents in ServiceNow without accessing it. In this case, the chatbot asks the user ID and a short description of the issue. The user ID is validated before being sent to ServiceNow API together the short description. The Affected user of the incident will be the user user ID provided, the Created by, Opened by and Configuration item will be the generic ones created for the chatbot.

There are other types of contact available for selection when creating an incident using ServiceNow, but they are not applicable for the channels currently available in CNHi.

4.4 *Classification and Initial Support*



Picture 12 - Process of Classification and Initial Support of Incidents (Source: Drive IT Global Services, Incident management Process Guide, 2015)

During the initial logging, incident category, symptom and sub-symptom is allocated so that the exact type of incident is recorded. This is important to route the ticket to correct resolver group and when analyzing Incident types and frequencies to establish trends.

Incident categorization may change throughout the lifecycle of an incident. For example, upon later analysis, categories may reflect the actual Configuration Items at fault such as ‘server’ or ‘disk drive’. For this reason, the Incident record must be maintained as insight progresses.

Another important aspect of logging every incident is to agree and allocate an appropriate prioritization code. Prioritization can normally be determined by taking into account both the urgency of the incident, being how quickly the business needs a resolution, and the level of business impact the Incident is causing. In ServiceNow, Priority is automatically set based on Impact and Urgency according the table below:

Table 6 - Matrix Impact and Urgency x Priority

Impact	Urgency	Priority
Low	Any	P3 - Low
Medium	Low	P3 – Low
Medium	Medium or High	P2 - Medium
High	Low	P2 - Medium
High	Medium or High	P1 – High
Very High	Low or Medium	P1 – Medium
Very High	High	P0 – Critical

When the incident has priority P1 or P0, it is called major incident and there is a special process of communication to make aware all the needed stakeholders and keep them in touch until get a resolution. However, major incidents are not scope of this work and it will not be detailed in its specific communication process.

The analyst involved must carry out initial diagnosis, typically while the user is still on the telephone (if the call is triggered in this way) to try to discover the full symptoms of the Incident and to determine exactly what has gone wrong and how to correct or who can support correcting the issue. It is at this stage that diagnostic scripts and known error information can be most valuable in allowing earlier and accurate diagnosis.

In some cases, other users may have already reported the same incident and only a parent incident must be updated. The other incidents reported should be set as child of the main one. In other cases, the incident is a known error with a known workaround that can be suddenly provided, and incident closed. The analyst may resolve an incident while the user is still on the phone and close the incident if the resolution and recovery are agreed to be successful.

After the ticket registration and classification be completed, if the ticket is a new issue and there is no available workaround, it's assigned to a resolver group for investigation. This assignment can be manual, but it is normally automatic in ServiceNow, based on routing rules.

4.4.1 Routing Rules

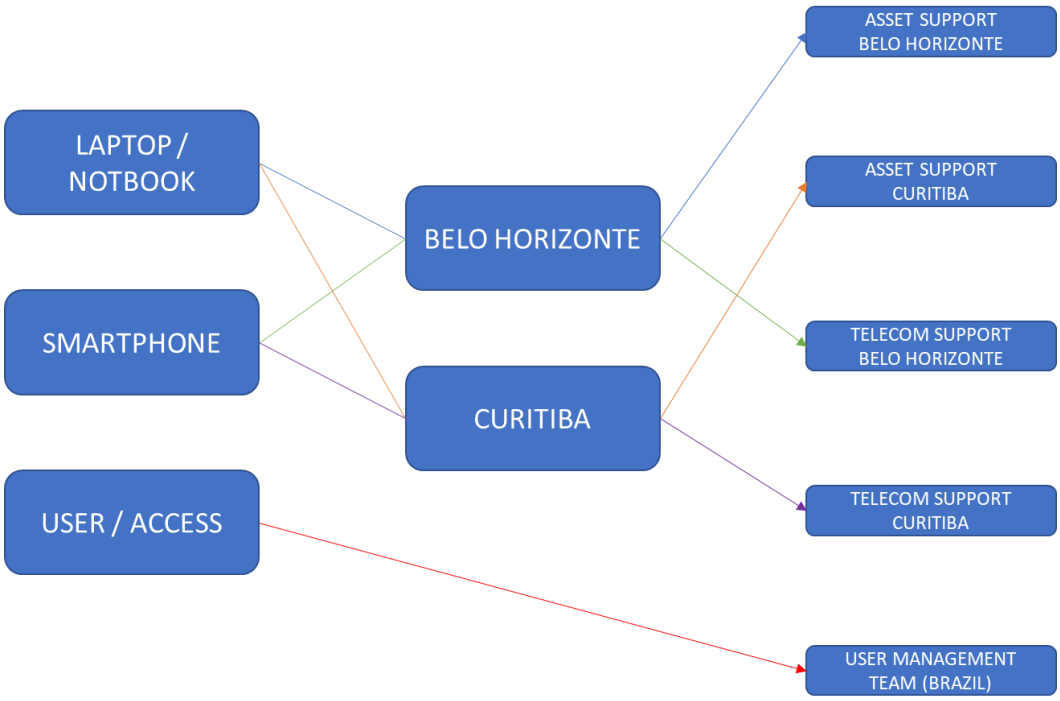
It worth it to dedicate a small section to explain better a powerful feature of the ServiceNow platform. For a long time, tickets were assigned manually by Service Desk analysts following scripts according user and ticket characteristics. For example, tickets about

network issue were assigned to the network team queue. In some cases, inside this team there were still reassignments to local groups, according user location. All this process used to take time and be likely to human mistakes.

ServiceNow platform introduced the concept of routing rules that automatically assign tickets to resolver groups according user, configuration item and issue characteristics. Basically, the scripts that usually were manually followed by SD agents, now are executed by the system, based on previously configuration.

If a service or application is supported by only one group, the field Support Group can be configured in the configuration item itself and all incidents created for this CI will be routed to that group. If the same service (e.g. Network) is shared among companies, regions and locations, with different support teams, routing rules can be configured based on the submitter location and company, for example. There are other characteristics that can be used to define the assignment group of the incident like the symptom of the fault or the type of the user. For example, all the tickets with VIP Affected User can be routed always to an executive support group, regardless any other characteristic.

A simple scheme exemplifying how routing rules work in ServiceNow platform can be see below:

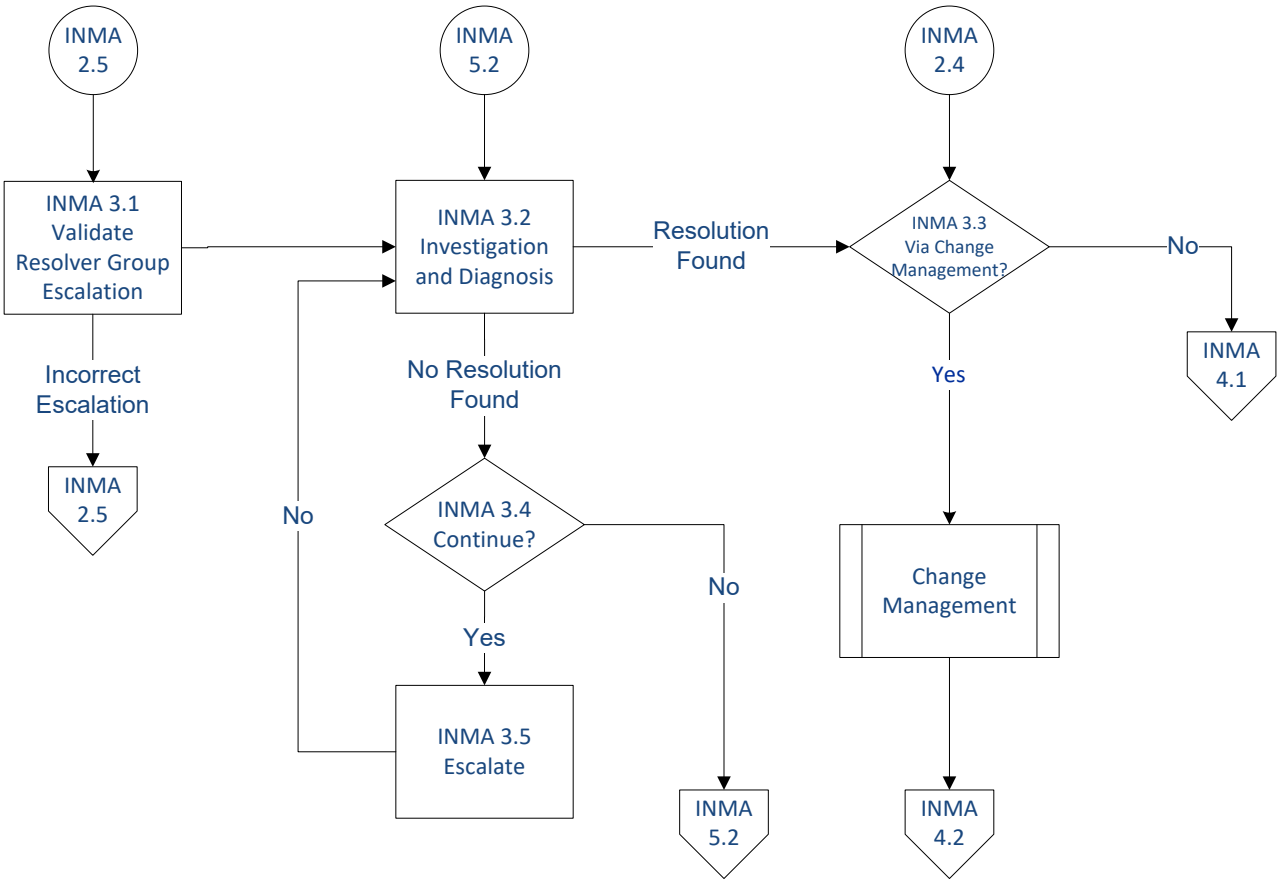


Picture 13 - Example of routing rules scheme on ServiceNow

By this scheme, if an end user from Belo Horizonte report a fault in his laptop, the ticket will be assigned to the team responsible for asset support in Belo Horizonte. On the other hand, if the user is facing an issue with his smartphone, the team responsible for telecom support in Belo Horizonte will handle the incident. The same logic is valid for users from Curitiba. Generally, if the user has empty location or a location without a configured routing rule, there is a higher-level routing rule to assign the ticket to a more generic group, responsible to reroute it.

In the case of incidents related to user or access management, by the scheme above, all the tickets would be assigned to a single group: User Management Team (Brazil). But other characteristics may be used, like country or company. In any case, the system always tries to match the ticket with routing rules from the most specific to the more generic.

4.5 *Investigation and Diagnosis*



Picture 14 - Process of Investigation and Diagnosis of Incidents (Source: Drive IT Global Services, Incident management Process Guide, 2015)

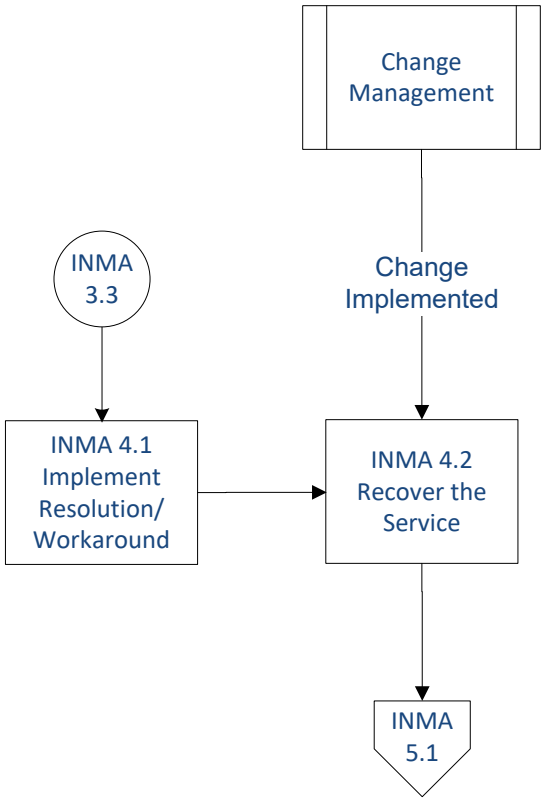
The first thing the resolver group assigned to a ticket should do is to confirm if this ticket should be assigned to it. The assignment can be manually done – thus likely for human error – or automatically routed – and susceptible to incorrect configuration. The automatic routing depends also in many cases of user data and if it is not complete and correct, the ticket can be incorrectly assigned. A ticket not assigned to the correct group is so called misrouted. When facing a misrouting, a member of a resolver group should reassign the ticket: to the correct group if he knows it, or to the group responsible to deal with misrouted tickets (usually the Service Desk). In both cases, the agent must mark the ticket as misrouted using the appropriated flag.

A reported incident requires investigation and diagnosis. Each of the support groups involved with the incident handling will investigate and diagnose what has gone wrong and all such activities (including details of any actions taken to try to resolve or recreate the incident) should be fully documented in the incident record as work notes so that a complete historical record of all activities is maintained at all times. Any communication with the affected user must be done via Additional Comments or, if done using other channels, logged in the incident record as an additional comment.

Even if it is possible to have only one group and analyst assigned to the incident record per turn, where applicable investigation and diagnostic actions should be performed in parallel to reduce overall timescales, however parallel actions need careful coordination, particularly resolution or recovery activities, otherwise the actions of different groups may conflict or further complicate a resolution!

This stage is one of the primary areas where Workarounds are located or developed. Escalations to other support groups may occur at this point. The Support levels assigned the incident will review the details, analyze to diagnose, and identify the appropriate course of action to resolve as quickly as possible. When an incident is not resolved, it is escalated to the appropriate support level.

4.6 *Resolution and recovery*



Picture 15 - Process of Resolution and Recovery of Incidents (Source: Drive IT Global Services, Incident management Process Guide, 2015)

When a potential resolution has been identified, it will be applied and tested. The specific actions to be undertaken and the people who will be involved in taking the recovery actions may vary, depending upon the nature of the fault, but could involve:

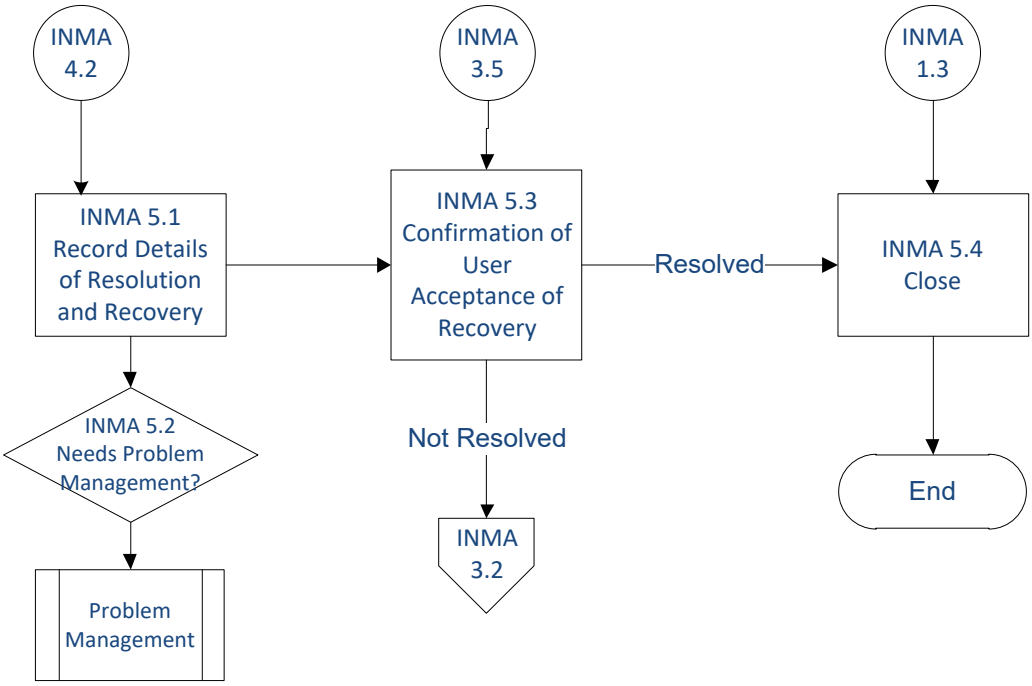
- asking the affected user to undertake directed activities on their own desktop or remote equipment;
- implementing the resolution either centrally (say, rebooting a server) or remotely using software to take control of the user's desktop to diagnose and implement a resolution;
- specialist support groups being asked to implement specific recovery actions (e.g. network support reconfiguring a router);
- a third-party supplier or maintainer being asked to resolve the fault.

Even when a resolution has been found, sufficient testing must be performed to ensure that the recovery action is complete, and that normal state service operation has been restored. In some cases, it may be necessary for two or more groups to take separate, though perhaps coordinated, recovery actions for an overall resolution to be implemented. In such cases

Incident Owner must coordinate the activities and liaise with all parties involved. Regardless of the actions taken, or who does them, the incident record must be updated accordingly with all relevant information and details so that a full history is maintained.

When updating an incident to Resolved state, the agent is asked to fill in mandatory fields informing if the incident was effectively resolved or not, and the solution provided and what caused the fault. These fields are closed list with pre-defined values, what possibilities reporting to analyze trends and identify improvement opportunities.

4.7 *Closure*



Picture 16 - Process of Closure of Incidents (Source: Drive IT Global Services, Incident management Process Guide, 2015)

After the incident is moved to Resolved state, it can be manually or automatically closed. The Incident Owner (or the Incident Analyst) can check that the incident is fully recovered and that the users are satisfied and agree the incident can be closed. The analyst should also check the following:

- Closure categorization - Check and confirm that the initial incident categorization was correct or, where the categorization subsequently turned out to be incorrect, update the record so that a correct closure categorization is recorded for the incident – seeking advice or guidance from the resolving support group(s) as necessary.

- Confirm the Close Code, Resolution and Causal Code details regarding to what was done to resolve the incident and update them if it's necessary.
- Incident documentation – Chase any outstanding details and ensure that the incident record is fully documented so that a full historic record at a sufficient level of detail is complete.
- Formal closure – Formally close the incident record.

If the incident is not manually closed within five days, it's automatically closed by the system. In any case, when the incident is closed, a survey is automatically sent by email to the affected user to give him/her the opportunity to evaluate the quality of the service provided.

5 Methodology

The project was organized in four parts:

i. **Literature Review:** review fundamental concepts of Information Technology Service Management, focusing on ITIL best practices and Service Now tool.

ii. **Data collection and analysis:** monthly data collected of all incidents closed by EUS groups in CNHi from October to January (four months). These data were analyzed to identify behaviors, patterns and trends.

iii. **Present and discuss results:** driven by outputs taken from data analysis in the step two, information was presented to global and regional responsible for the incident management process in CNHi. Investigations in the processes and interviews with responsible personnel were conducted to identify characteristics, regional differences and opportunities for improvements.

iv. **Delivery final report:** based on the outputs from step three, a report about the incident management process in CNHi was developed, highlighting regional aspects with advantaged and disadvantages of them. The report was delivered and presented to stakeholders to be used as support for decisions making to improve the ITSM processes in the organization.

6 *Discovering and analyzing the end user services*

Incidents are created in Drive IT all time through the four regions of CNH Industrial. Most of them are related to End User Services, which is the scope of this work. Understand the nature of this incidents, how they are reported and resolved is essential to evaluate the EUS in the company.

6.1 *The data collection*

The core objective of this work was to use the data available about the incidents managed in Drive IT to understand the processes and their differences between the regions, identify gaps, failures and improvement opportunities. In order to do that, reports to monthly collect these data were developed using the native report feature of ServiceNow platform. For each region, the Incident Manager (of scope EUS) provided a list with all the EUS resolver groups and a report was created to extract all incidents closed by these groups in the last month. The table incident contains innumerous columns and the following ones were included in the reports, based on the information relevant for this work:

Table 7 - Fields included in the incident monthly report

Field	Description
Created	Date and time when the incident was created.
Number	A code that uniquely identify the incident.
Short description	A brief description about the issue.
Configuration item	The configuration item affected by the incident (e.g. an application or service).

Contact type	The type of contact the affected user utilized to report the issue.
Affected user	The user that was being affected by the incent.
Location	Location of the Affected User.
Priority	Final priority of the incident (automatically set based on impact and urgency).
Assignment group	The resolver group assigned to the incident when it was closed.
Assigned to	The member of the assignment group that was assigned to the incident when it was closed.
Causal code	The cause of the issue selected from a pre-defined list by the analyst when resolving the ticket.
Resolution	The resolution applied to the incident. It's a value selected from a pre-defined list.
Resolution and confirmation notes	Free text field where the analyst resolving the incident can provide additional information on the solution.
Resolved	Date and time when the incident was resolved (always populated with the last time when incident state was changed to resolved, even if it was reopened after first solution).
Resolve time	Difference in seconds between the Resolved and Created dates and times.
Reassignment count	How many times the incident was reassigned from a resolver group to another.
Resolved by	The analyst who resolved the incident (updated its status to Resolved).
Country	The country of the analyst that resolved the incident (the Resolved by).

Region	The region of the analyst that resolved the incident (the Resolved by).
Closed	Date and time when the incident was closed (state was updated from Resolved to Closed). An incident can be manually closed, or it is automatically closed after five days from resolution.
Close code	A code to determine if the ticket was solved or not solved.
Closure comments	Free text field where the analyst manually closing the incident must provide additional information on the closure. If the incident is automatically closed by the system, a default message informing this fact is added.

6.2 *Refinement and analysis of data*

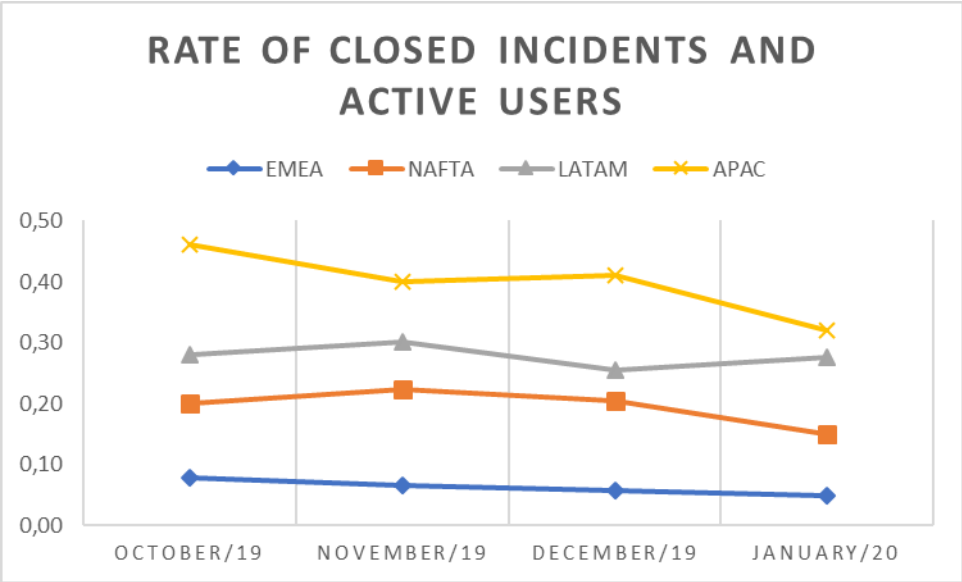
Every month, data extracted from the reports were exported to Excel, where they were refined and combined to provide valuable information. These information were not the same for all monthly analysis, because needs of information were being identified and modified during the work, as result of the presentations for the regionals Incident Managers and the Incident Process Manager.

The Incident Managers were required to list all resolver groups active for the End User Services in each region. Reports were done to extract all incidents closed in the first month of the analysis, October 2019. They were divided by regions and one of the information important to check was the volume of incidents closed in each one of them.

Picture 17 - Volume of incidents closed and number of active users in each region (October 2019)

Only the number of incidents closed cannot be conclusive or give a valuable information. A reason for a region closing more incidents than another can be a higher number of incidents due to the existence of more plants, for example. Thus, the information about how many active users the region had at the moment of data collection was added to the chart and a rate between quantity of users and tickets closed was calculated. Regions LATAM and NAFTA have similar rates, while EMEA and APAC are extremes with a very higher and a very lower value, respectively. Both EMEA and APAC closed more tickets than LATAM and NAFTA in October 2019, but the rates are largely different due to the number of active users. With about 40,000 users, EMEA had almost four times the number of users in LATAM and NAFTA. Looking to APAC users, the difference is even higher: one eighth of EMEA users.

In order to confirm these indicators, same report was generated in each month and for the two first months of data analyzed (October and November of 2019), there were not big differences in the individual rates presented by each region. On December 2019 there was a small decreasing in the volume of incidents in all regions, except APAC. The reason was that only in APAC the Christmas and End Year holidays were not celebrated. On the first month of 2020, there were significantly decreasing in NAFTA and specially APAC number of incidents closed. This may be justified by the Chinese New Year and extended vacation due to the epidemy of Coronavirus. These numbers are showed in the following chart.

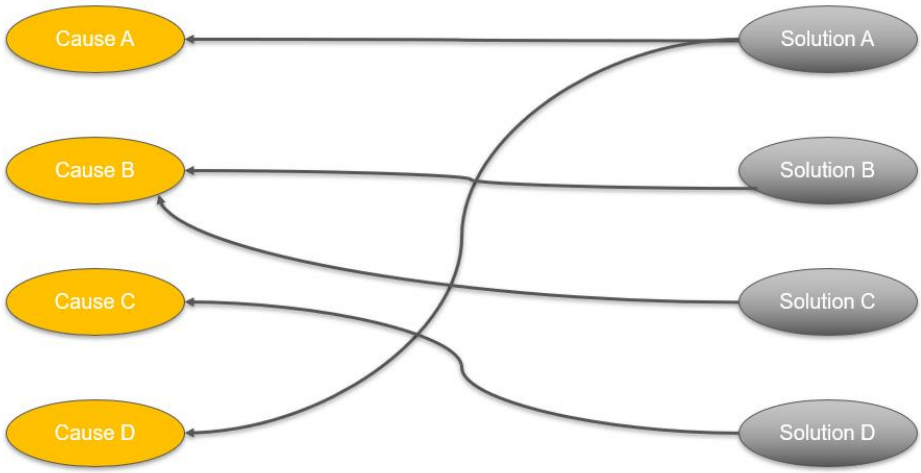


Picture 18 – Evolution of rate of closed incidents and active users by regions through the months

Why EMEA has so many users than other regions? Why APAC volume of incidents closed is higher than LATAM and NAFTA ones, even with almost half of active users than them? These were questions raised that answer could indicate differences in the process or even failures. Even if the differences in volumes of incidents of each region were interesting questions raised, the initial scope of the work was to try to reduce the volume of incidents in general. Thus, it was important to understand which incidents were those and how they were being resolved.

6.3 *Characteristics and resolutions of incidents*

Incidents are supposed to be reported with as much information as possible to let the support team to understand, replicate and resolve them. However, another very important activity made by the technicians is the classification of the incident. When resolving an incident, the technician must provide information about the nature of the incident and the resolution applied. In Drive IT, these are mandatory list fields with pre-determined values that were defined based on the most commons causes and resolutions for incidents. These classifications are very important to provide inputs for post analysis that can identify trends, behaviors and feed knowledge bases. The picture below shows a proposed analysis to try to map causes and resolutions:



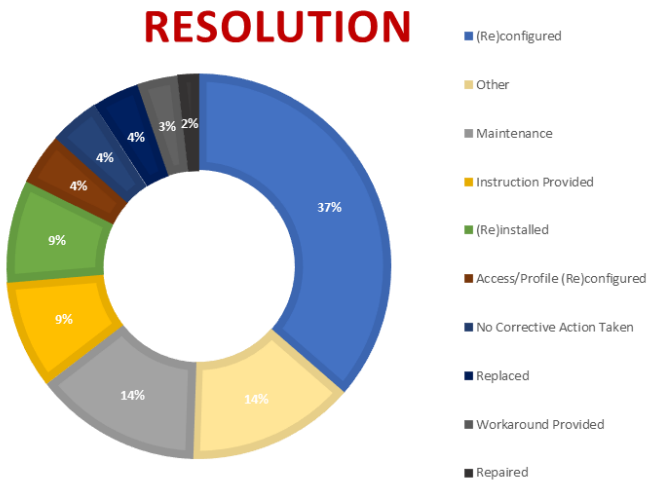
Picture 19 - Mapping causes and resolutions of incidents

Mapping causes and resolutions of incidents can be useful to identify commons cases of faults where known solutions or workarounds are frequently applied, and they may be documented in a knowledge article. A knowledge article is a page stored in a knowledge base where users or technicians can access to learn something. A knowledge article documenting a workaround for an incident that the end user could apply by himself without contacting the Service Desk may contribute to reduce the volume of incidents created. An example is the issue with password cached that the user would be able to clean the cache of his browser following instructions documented in a knowledge article. Even for the members of a support group, knowledge articles are useful to help them to improve the time of resolution of incident with know solutions for common issues. The following table shows examples of resolutions applied to causes of faults found in the data extracted from Drive IT.

Table 8 - Common causes and applied resolutions of incidents

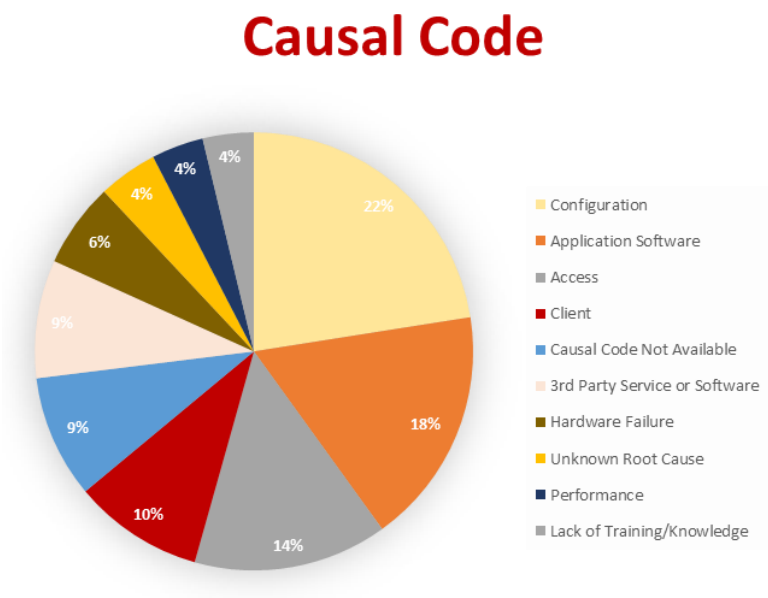
Resolution	Causal Code
Access/Profile (Re)configured	Access
	Password cached
Repaired	Hardware Failure
Replaced	
Instruction Provided	Lack of Training / Knowledge

This kind of analysis could be very beneficial, however it depends on something essential: the quality of data. The quality of the data is a result of the how well the agents are classifying incidents and their resolutions when they are resolving them. Unfortunately, looking to the data collected during the months when the analysis was done, it was observed the use of very generic classifications that doesn't valuable inputs for improving the process of incident resolution. As it can be seen in the chart below, the top 10 most used resolutions are almost all generic terms that alone doesn't mean very much.



Picture 20 - Top 10 Resolutions applied to incidents closed in December 2019

Only the resolution "(Re)configured" was applied to more than one-third of the incidents closed in the month December of 2019. This solution was the most applied also in all the other months analyzed. But what does it means configure or re-configure? What was (re)configured? And why? To answer those questions, it was necessary to analyze also the causes of the faults and the affected configuration items (applications or services). Maybe looking to these information together could be conclusive. The chart below shows the top 10 causes used to classify the incidents closed in the same month of chart before with top 10 resolutions (December 2019).

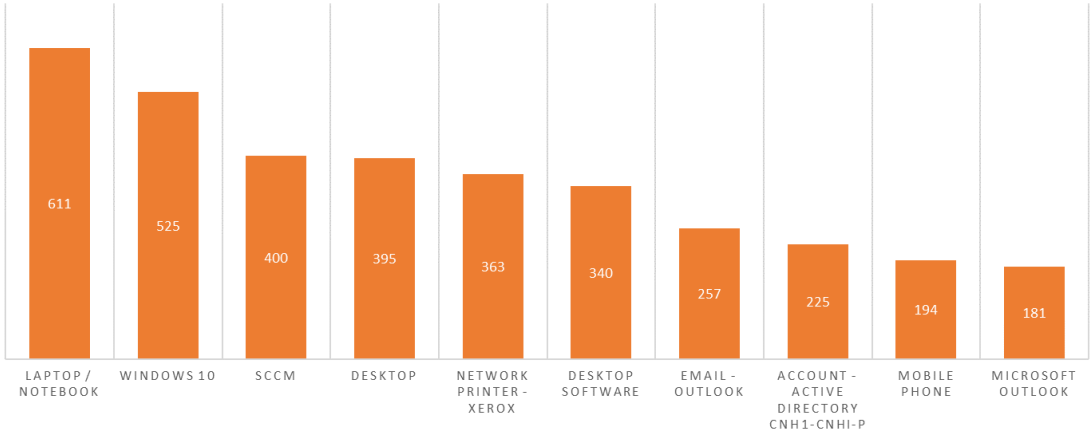


Picture 21 - Top 10 Causal Codes for incidents closed in December 2019

Defining what caused the incident doesn't mean to follow the formal process of root cause analysis present in the Problem Process of the ITIL library (not in the scope of this work). The Causal Code should, at least, inform the nature of the issue, even in a superficial way. Superficial but not that much as it was observed looking to the data collected. It is not surprisingly that if the most applied resolution was (re)configured, the most common cause of the issues was configuration. But which information can be extracted from this pair?

The causes "Causal Code Not Available" and "Unknown Root Cause" should be exceptions and rarely used, but they are in the top 10 of most used. If a causal code is not available in the existing list of the field, should it be added? For who the analyst should report it? Or is it a process in place to periodically evaluate those cases? What does it mean that the cause of the incident is unknown? It was not reproduceable? Was the analyst well trained to identify causes of failures?

The second most common cause used to classify incidents' nature was "Application Software". But was the software being affected by the incident or was the software causing the incident? And which is the software? If an application software is being affected by an incident, it should be set as its Affected CI. The next chart shows the top 10 most used configuration items as Affected CI by incidents closed in December 2019.



Picture 22 - Top 10 Affected CIs by incidents closed in December 2019

Many incidents closed in December 2019 were affecting hardware as it is shown by the CIs Laptop/Notebook, Desktop, Network Printer – Xerox and Mobile Phone. That is a useful information, but is it enough? Except for printers, all the other hardware are present in Drive IT as individual assets. If an end user reports a fault in his laptop, he – in case of using the self-service portal – or the Service Desk analyst must select the laptop from a list of assets assigned to that user. The generic CI should be used only in cases where the proper asset is not found. Having single assets as Affected CI for incidents could, for example, indicate issues more frequently with a specific manufacturer.

Other generic CI very used as indicated by the chart was Desktop Software. There are many software registered as single CIs that should be used instead of the generic one. Using the generic CI cannot indicate, for example, that many users are reporting issues with a specific application or even a version of it. Moreover, the nature of issues and their resolutions can vary from an application to another. An application that shows up as a single CI in the top 10 is Microsoft Outlook. However, considering that is also present in the top 10 the CI "Email – Outlook", it is not clear if both these CIs were used to indicate issue in the service of emails or if the first one was used to signalize issues in the application and the second one to indicate faults in the service. There is also a third CI very used for email services that is "Email Client – Outlook". What are the differences between these three CIs? Are the teams and users aware and aligned on it through the four regions?

Even if there are common characteristics in the incident management through the regions, it was already showed that there are also differences between them. An example was the rate of incidents and users discussed in the section 6.2 and another one was the types of contacts used by the users to report incidents that was showed by Picture 5 in the motivation

section of this report. In order to understand better the incident management in all CNHi it is essential to deepen on these specifies of each region.

6.4 *How each region manages incidents in CNHi*

Analyzing the data of incidents has provided valuable information to understand especially how users report issues and how the support teams resolve them through the different regions in CNHi. Not only the channels used by users to contact the support teams – as already showed – are different, but also the way the incidents are initially assigned and then managed until they get a resolution. These differences – that had never been raised and discussed before – surprised even the global Incident Process Manager of CNHi. To present the differences and how it was possible to identify them, they will be divided in three sections:

1. How incidents are logged in CNHi
2. How incidents are managed in CNHi

6.4.1 How incidents are logged in CNHi

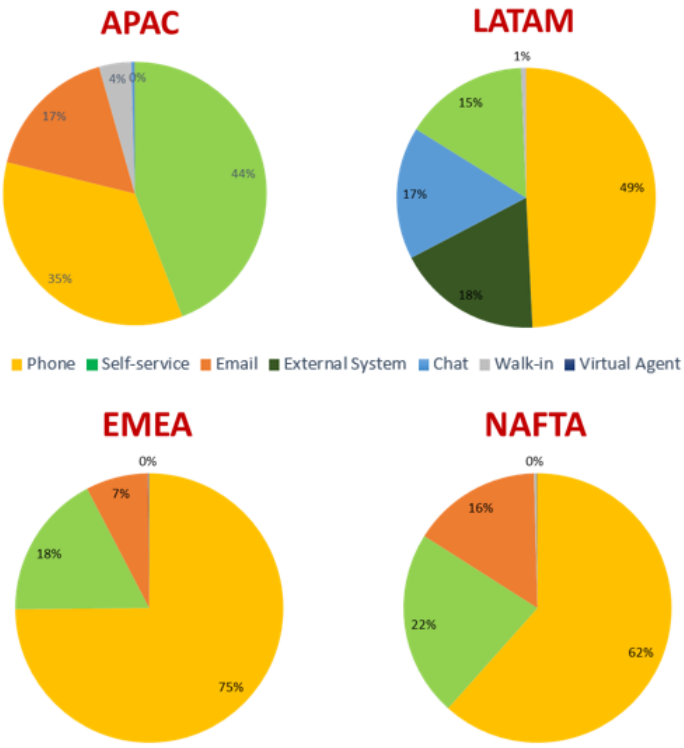
In different companies, there are many options an employee or collaborator can use to report issues to technical teams in order to receive support. From walk-in (going to talk physically with a technician) to telephone calls or internal chats, for example. Each company, in agreement with its suppliers, provides users a list of defined available channels. In CNHi it's not different, but it's not even the same for all regions. Each individual region makes available different channels for users to contact suppliers and receive support.

The types of contact enabled in Drive IT were defined according the use in FCA and CNHi. Analyzing the incident data and discussing them with regional Incident Managers, it was possible to identify the available channels in which region of CNHi:

- APAC: Self-service, Phone, Email, Chat and Walk-in
- EMEA: Self-service, Phone, Email, Chat and Walk-in
- LATAM: Self-service, Phone, Chat, Walk-in and Virtual Agent
- NAFTA: Self-service, Phone, Email, Chat and Walk-in

The share of incidents created by each one of these contact types among the regions were already showed for the October 2019 – the first month of data collection – in the Picture 5 in the Motivation section. For all regions, Chat and Walk-in were very rarely used, with percentages close to 1% or even zero. For EMEA and LATAM, the Phone contact was by far the most used, with about three-fourth of all the incidents for both. APAC and NAFTA use significantly the Phone contact too, but they also often use Email channel (that is also available, but not very used, for EMEA). The Self-service contact was reasonable present for all regions, with about 20% for EMEA, LATAM and NAFTA. In APAC, this type of channel appeared as the most favorite for end users to report issues. However, in the first meeting with the regional Incident Managers it was identified that it was a fault in the process of ticket creation in APAC, where SD agents were not correctly setting the contact type.

Except for LATAM, during the four months of analysis, the shares of contact type for each region did not present big variations. In APAC, the issue with contact type categorization was not fixed, in EMEA, the telephone continued to be responsible for about three-fourth of the incidents reported and NAFTA had small variations between telephone and email, but keeping both as most used channels. The results of last data collection – from January 2020 – can be seen in the charts below.



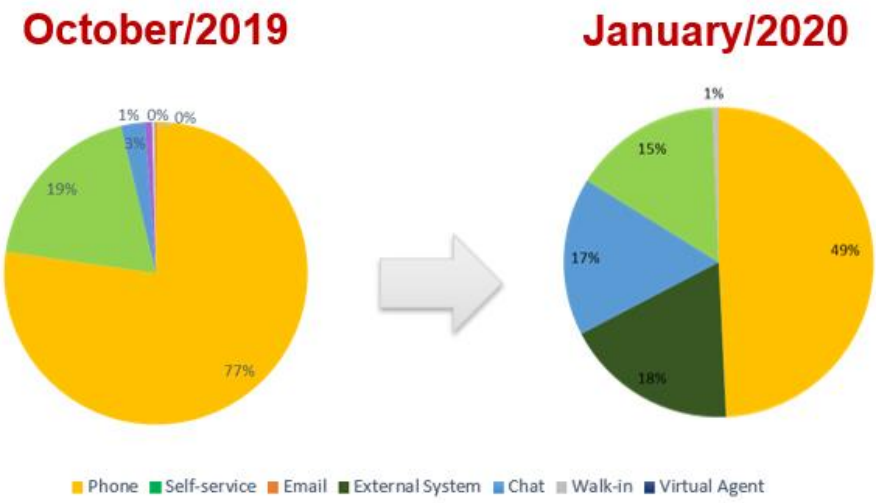
Picture 23 - Type of contact used by region (January 2020)

Since the second month of the analysis, LATAM region had already presented a decreasing in the percentage of Phone contact type and, on the opposite way, an increase in contact types External System, chat and Walk-in. Presenting the data in the meeting with all regional Incident Managers and the global Incident Process Manager, it was explained by LATAM responsible that these variations were resulted by three initiatives:

- The launch of the chatbot **Ceni Dutra**: Ceni Dutra was a chatbot based on Sophie virtual agent – a solution provided by Stefanini – that was already used in the legacy ITSM platform used by CNHi LATAM before going onboard to Drive IT. The chatbot, active on Skype for Business, was migrated to Drive IT, doing the integration via API. Ideally, the type of contact for incidents created using Ceni Dutra should be classified as Virtual Agent, but it was identified that they were using External System.
- Enable **WhatsApp** as a channel to contact the Service Desk: a WhatsApp number was made available for users as an alternative way to contact the Service Desk, instead of doing phone calls. The intention of this new channel was to streamline the calls and use better the resources, since a single SD agent can take in charge more than one WhatsApp message at the same time, while phone calls are exclusive. For any WhatsApp contact received, agents should follow the same process for phone calls on Drive IT: create a call record and then, if it is the case, create an incident. The difference is in the contact type: for WhatsApp contact it is classified as Chat.
- Installation of **Walk-up Locations** (or Tech Stops): in two sites in Brazil – Contagem and Sorocaba - there were installed physical Walk-up locations (also called Tech Stops) where users can bring their computer, mobile phone or any other device there and receive support on site. Users can book an appointment or go the Tech Stop and do the check-in there (subject to eventual line). Both appointment and check-in generate a walk-up interaction that should be assigned to a technician working in the Tech Stop. If the support is related to an issue, the technician must create an incident from the interaction and classify its contact type as Walk-in.

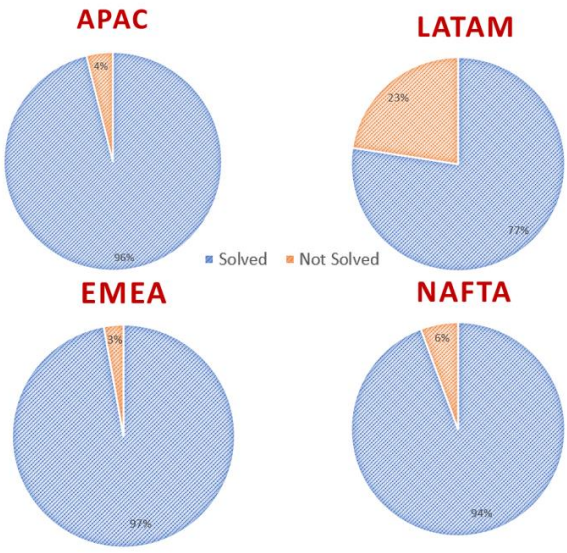
These initiatives were implemented as part of the LATAM plan to reduce in 70% the number of telephone calls to the Service Desk by the end of 2020. In LATAM, most of the

work done by the Service Desk agents is only to dispatch, receiving calls and creating tickets that are already automatically assigned to proper groups thanks to routing rules. The small volume of issues resolved by the Service Desk agents as first call resolution is wished to be done by the virtual agent in the future. The final goal is to eliminate the Service Desk level 1 and have the virtual agent as the only channel for users to report issues. If the virtual agent cannot resolve the issue with tips and knowledge articles, then it can create the incident in Drive IT (that will be automatically assigned to a proper level 2 support group according the routing rules). In three months, LATAM has already overcame more than a half of its goal for 2020, reducing the volume of telephone calls to the Service Desk in about 36%, as it can be seen by the picture below:



Picture 24 - Evolution of shares of contact type for incidents in LATAM

Initially, only looking to this chart, it is possible to say that LATAM is going pretty well in its goal to reduce – and finally – eliminate the Service Desk. However, it is necessary to evaluate also the alternative tools provided for end users to report incidents. Analyzing the resolution of incidents, it was identified an indicator of anomaly in LATAM.



Picture 25 - Close code of incidents by region (incidents closed on November 2019)

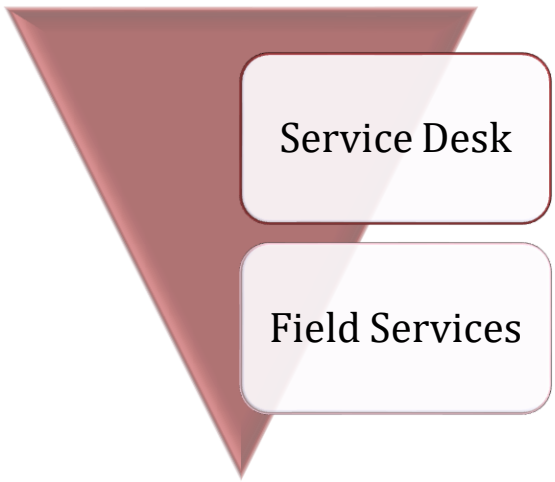
When the agent resolves and incident, it is mandatory to inform the Close code, choosing from four options: Solved, Not Solved, Cancelled or Not Reproduceable. For analysis purpose, last three were grouped in Not Solved only. Looking to these charts it is easy to observe that LATAM had much more not solved incidents than other regions. Presenting them to the regional Incident Managers, it was identified that the high volume of not solved incidents in LATAM was most originated by cancelled tickets incorrectly created by users using Ceni Dutra (the virtual agent). Most of them were users requesting printing quota, that is something users were habituated to do when Ceni Dutra was integrated with the old ITSM platform used by LATAM before going on-board to Drive IT. Since printing quota are service requests (another type of ticket), all incidents created by users using Ceni Dutra with this intention were being cancelled by the SD. This raised an improvement opportunity on the virtual agent and better orientations to end users. Results of actions could be observed by the evolution of solved incidents created using Ceni Dutra:

Picture 26 - Evolution of solved incidents created using the virtual agent in LATAM

During the period of analysis were also observed incidents in regions like APAC that were not resolved and should be closed as cancelled by were closed using the close code Solved. Thus, another possible reason for having LATAM with a higher share of not solved incidents can be that other regions are not properly using the close code. From the analysis, in many points, LATAM was the region presenting more differences. The type of contact was just one of them. Other regions are still dependent of a central Service Desk, where tickets that cannot be resolved by them are manually routed to proper groups, because they did not configure routing rules based on configuration item and user location, as it was done for LATAM. What are the reasons for these differences? How each region manages their incidents to have them resolved?

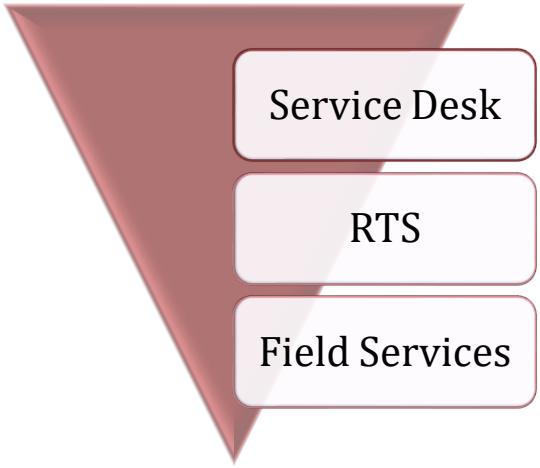
6.4.2 How incidents are managed in CNHi

Not only the way incidents are reported and logged in Drive IT is different among the regions, but also the way they are managed. One more time, the region presenting a more different process is LATAM. For APAC and NAFTA, most of the incidents are reported by telephone calls or email messages and, in both cases, a Service Desk agent should take the call or email in charge and register it on Drive IT. Even when users report the issue by themselves using the self-service portal, the incident is assigned to the central Service Desk, regardless user location. This central Service Desk is the first level of support and it is responsible to try to resolve as much incidents as they can (especially simple issues). When the SD agent is not able to resolve the issue, he or she reassign the incident to the level 2, which can be another remote team or a field one (when it is necessary to go physically on the user's desk). The intention of this model is to avoid engaging specialized and local teams and having a remote and central Service Desk resolving as much issues as they can.



Picture 27 - APAC and NAFTA End User Services model

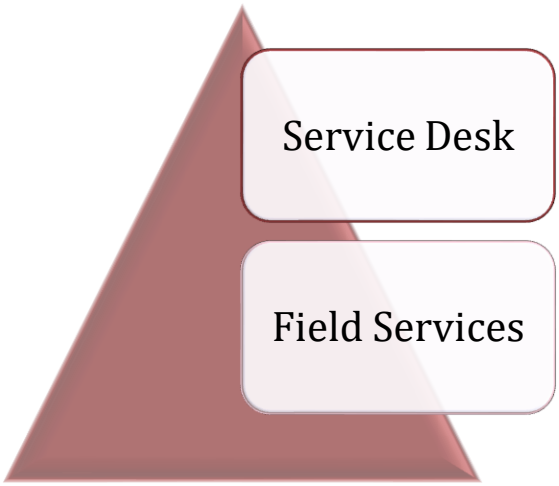
EMEA region has added a middle layer between first and second level of support, respecting to APAC and NAFTA. First point of contact is still the Service Desk – mainly by telephone – and the goal is to resolve most of the tickets in that support level 1. If the SD agent cannot resolve the issue, before routing it to a field team, the ticket is assigned to a kind of level 1.5 of support called Remote Technical Support (RTS). If this more specialized group is also not able to resolve the issue, then it is routed finally to a field team.



Picture 28 - EMEA End User Services model

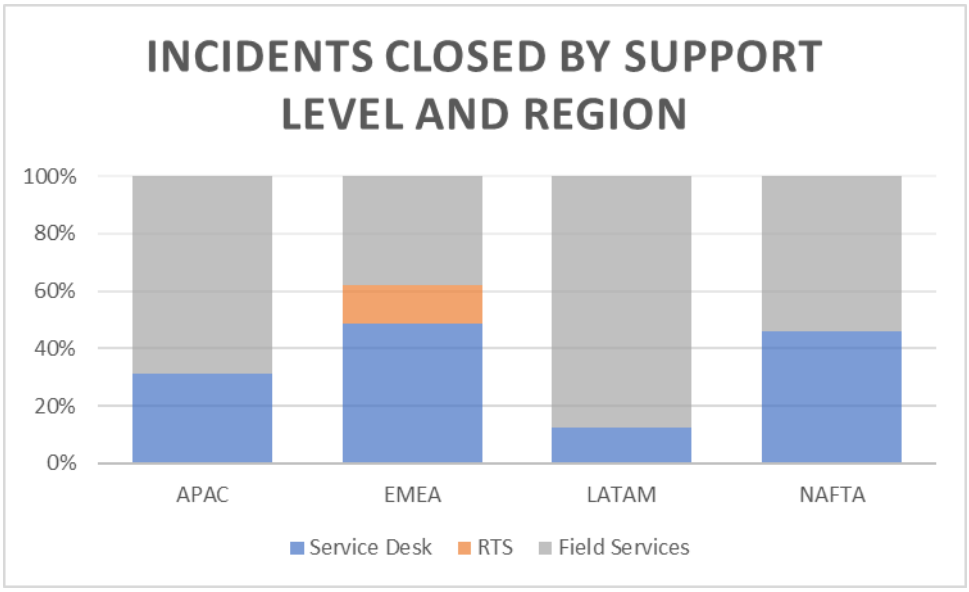
In South America region (LATAM) the EUS services were modelled in a different way: local technicians are responsible for the higher volume of tickets. The Service Desk in LATAM also do a kind of first level of support, but resolving simpler issues than Service Desk does in other regions. In LATAM, the main function of the Service Desk is to receive calls and log tickets. These tickets registered by the Service Desk are automatically assigned to a specialized

team (in most cases a local one) that is responsible to resolve them. Since in LATAM the Service Desk has this very limited job of registering that can be done by the user himself (via portal) or other tools (like a virtual agent), the regional team implemented and encouraged people to use alternative channels to the Service Desk to report issues.



Picture 29 - LATAM End User Services model

These different models of managing EUS tickets were not well known among the regions, specially the LATAM one. It was possible to identify and understand them thanks to outputs provided by data analyzed about tickets closed by groups from each region.



Picture 30 - Incidents closed by support level and region (incidents closed from October 2019 to January 2020)

From this chart it would be possible to conclude that the pairs APAC and LATAM, and EMEA and NAFTA should have similar EUS models. However, analyzing the data together

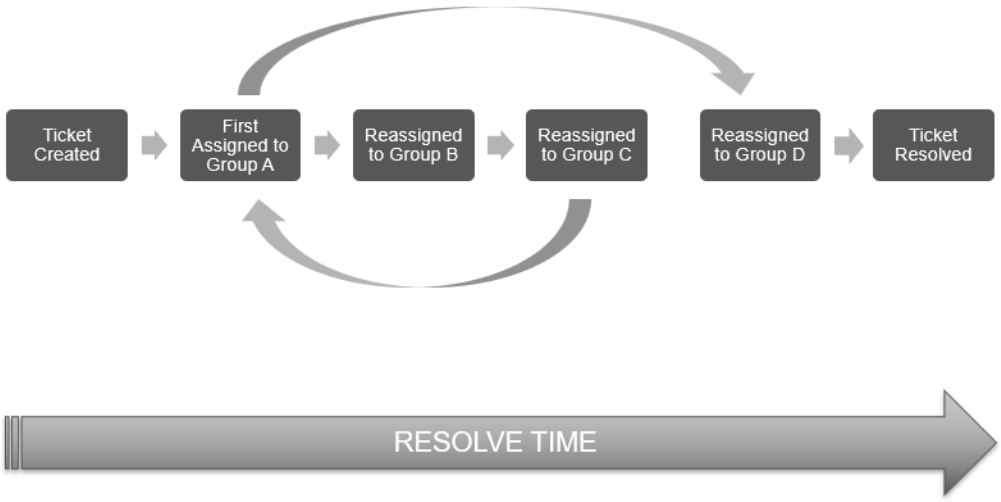
the regional Incident Managers, it was explained that LATAM has a very different way to manage tickets, but APAC does not. In the case of APAC, the model is the same followed by NAFTA and the volume of incidents resolved by the Service Desk ideally should be much higher. For APAC, this result can be an indicator of an improvement opportunity, like Service Desk needing training or procedures and orientations.

EMEA and NAFTA had similar share of incidents resolved by the Service Desk (about half of them), but considering the middle layer RTS, the first region achieves 60% of the incidents resolved without engaging a field team. NAFTA, like the other two regions (APAC and LATAM), presents also incidents resolved by other groups that were not classified as Service Desk neither Field. The classification of groups was done together the regional Incident Managers. Service Desk is the first level of support and any support level 2 like specialized or allocated teams are considered Field Services.

If a ticket can be resolved by a central and remote Service Desk, its resolution can be faster and cheaper than if the engagement of local and specialized team were necessary. On the other hand, if the Service Desk cannot resolve an issue and need to route it to another team, at least two agents were already engaged and, then, resolution probably will cost more and be slower than if the ticket were initially assigned to the proper group. Then, what is the best model to adopt? Is it possible to combine resolution speed for the end user and costs reduction for the company? How to define, measure and control an ideal End User Services model?

6.5 *Evaluating the resolution of incidents*

The performance of suppliers providing IT services are measured by Service Level Agreements (SLAs) that are defined in contract by each region and its suppliers. These SLAs are configured in Drive IT and managed using reports and dashboards that are normally presented in periodic meetings between regional leaders and suppliers. Specific SLAs are configured for different groups considering the nature of the service, the availability of the support, location of suppliers (and its time zone and local holidays), and other specificities that vary from one support group to another. It is not the purpose of this work to explore the SLA subject, due to its complexity and differences among regions. To evaluate how each region is resolving incidents for End User Services, two characteristics of incidents were analyzed: number of reassignments and time to resolve.



Picture 31 - Number of reassignments and resolve time

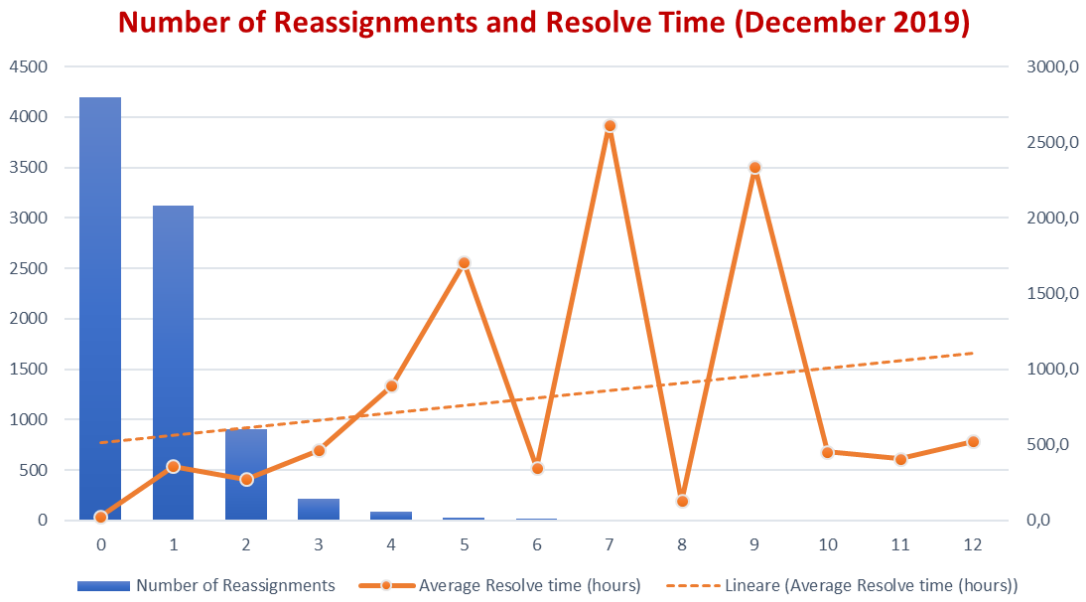
When an incident is created, it is initially assigned to a resolver group that is responsible to fix the issue or provide the user a workaround. The assignment is done based on ticket and user's characteristics like application or service with issue and location of the affected user. In LATAM region, many routing rules were configured to automatically assign the tickets and the core criteria used by them was the user location. This is aligned with the model adopted by the region, having the local groups of technicians as the main source of support. Other regions did not implement routing rules based on locations and the default initial assignment group for EUS configuration items is the central Service Desk. If the level 1 support is no able to resolve the issue, the ticket is manually reassigned to another group. The Service Desk agent in charge of the incident reassign it following orientations that consider similar criteria of automatic routing rules configured for LATAM.

Either automatic and manual assignment are subject to make mistakes and incorrectly route a ticket to a not proper group. This event is called misrouting and should be flagged using the existent flag for this purpose. However, looking to the collected data, it was observed that no region was using it. There was a gap on how to deal with misrouted tickets. From regional Incident Managers' explanation, the only orientation for group members receiving incorrect tickets were to reassign them to the central Service Desk for proper routing. This a reactive action, however proactive actions are also needed in those cases like to investigate why the ticket was incorrectly routed before: issue with routing rules configuration? Missing user's data? Lack of knowledge of SD agent?

In any case, every time an incident is reassigned, a field on incident table called Reassignment count is increased by one. Looking to this field, it is possible to know how many

times an incident was reassigned before getting resolved. This number can be an indicator of the quality of service provided, because every time an incident is assigned to a group, an additional agent is being engaged. Moreover, tendency, as more a ticket is routed from a group to another, longer is the time to get it resolved. This time of resolution for each incident is recorded in seconds in the field Resolve time. It is a simple calculation subtracting the dates and time when incident was resolved and when it was created. It does not consider business time, holidays and incident states, but it can be used and analyzed as an indicator of performance for all regions.

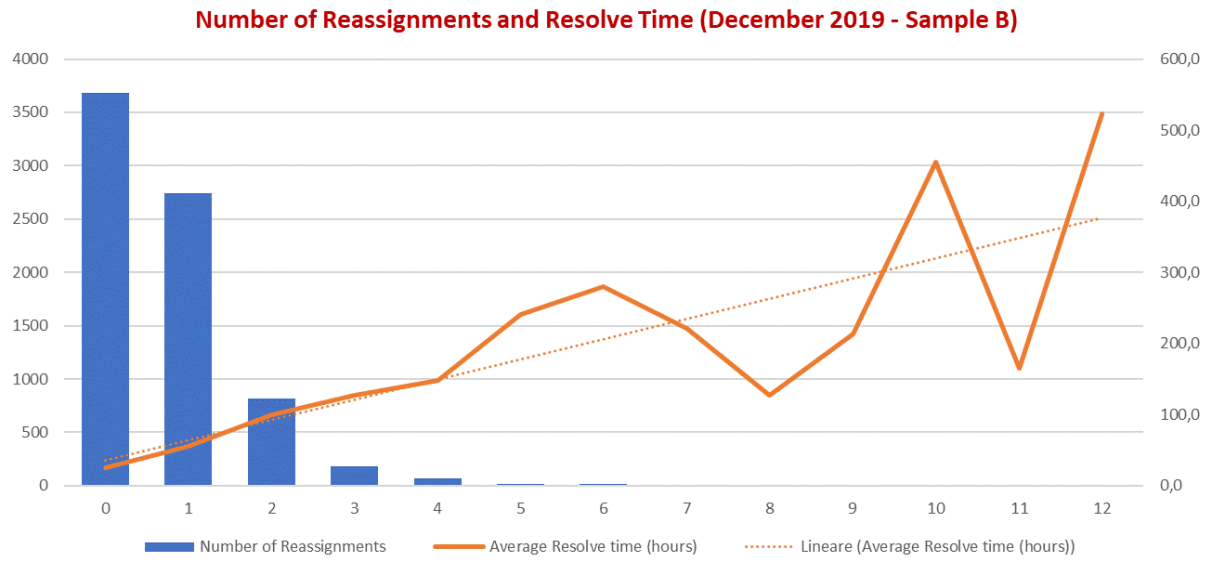
These two indicators – number of reassignments and resolve time – were analyzed together to try to prove that they are related and to evaluate each single region based on them. Its first analysis was done using data of incidents closed on December 2019 and a result can be seen in the chart below.



Picture 32 - Number of reassignments and resolve time (incidents closed on December 2019)

In the horizontal axis of the chart, there are the number of reassignments that were observed in tickets closed on December of 2019. The bars show – using the main vertical axis (on the left) the quantity of tickets that had each number of reassignments. The average of resolve time (in hours) is showed by the line and the secondary vertical axis (on the right). Even if there are sparse points, it is possible to see a tendency showed by the draw line that as higher the number of reassignments, longer is the average of resolve time. But what are these sparse points?

An outlier is an observation that lies outside the overall pattern of a distribution (Moore and McCabe 1999). Outliers should be removed from the sample and analyzed separately. In this case, outliers can be tickets opened for a long time and closed in the month data was collected, tickets logged as a retroactive action (to register a task already completed), or other situations out of the normal execution of the process. To remove the first two cases, it was defined together the Incident Process Manager to exclude from the sample tickets with resolve time longer than one month and shorter than two minutes. 1047 items were excluded from the original sample of 8592 incidents, keeping thus about 88% of the sample. Then, the same chart was plotted again:

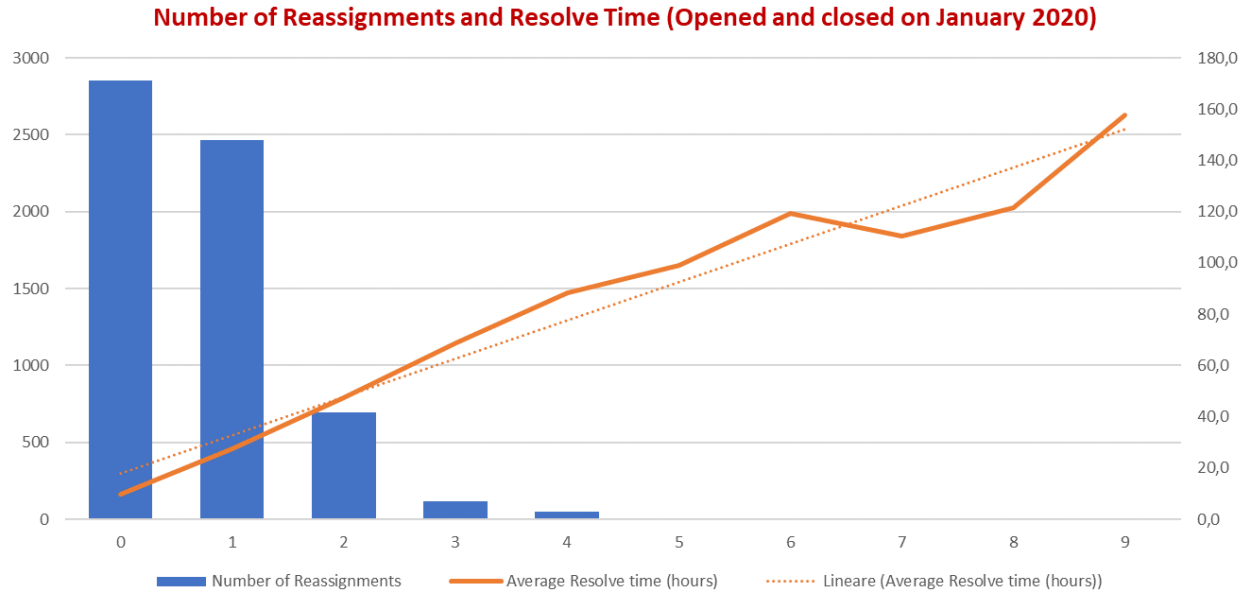


Picture 33 - Number of reassignments and resolve time (incidents closed on December 2019, sample B)

This second chart shows an even stronger tendency to have longer resolve time for tickets with higher number of reassignments. Variation can be from less than 50 hours for incidents with one or no reassignment to more than 400 hours for incidents reassigned 12 times or more. There are still some small outliers, like for incidents with reassignment count equal to 8 or 11, but it may be because being the number of tickets with this quantity of reassignments small, any variation has more power to affect the amplitude of the average.

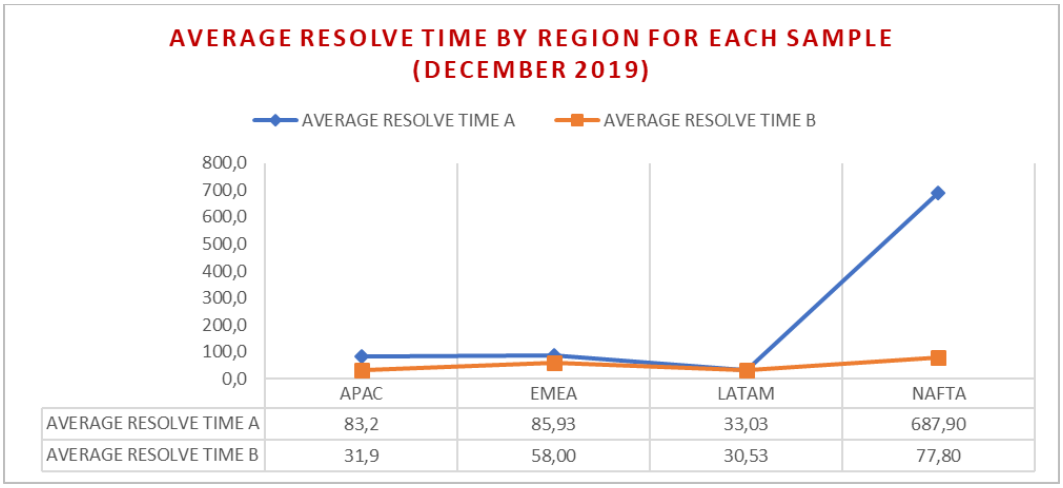
The same analysis was repeated for incidents closed on January 2020 and the tendency of having longer time to resolve with increasing number of reassignments was confirmed. To simulate a scenario closer to what happens with most of the tickets, a chart was plotted

considering only incidents opened and closed in January of 2020 and, after removing outliers, result was similar, as it can be seen below.



Picture 34 - Number of reassignments and resolve time (incidents opened and closed on January 2020)

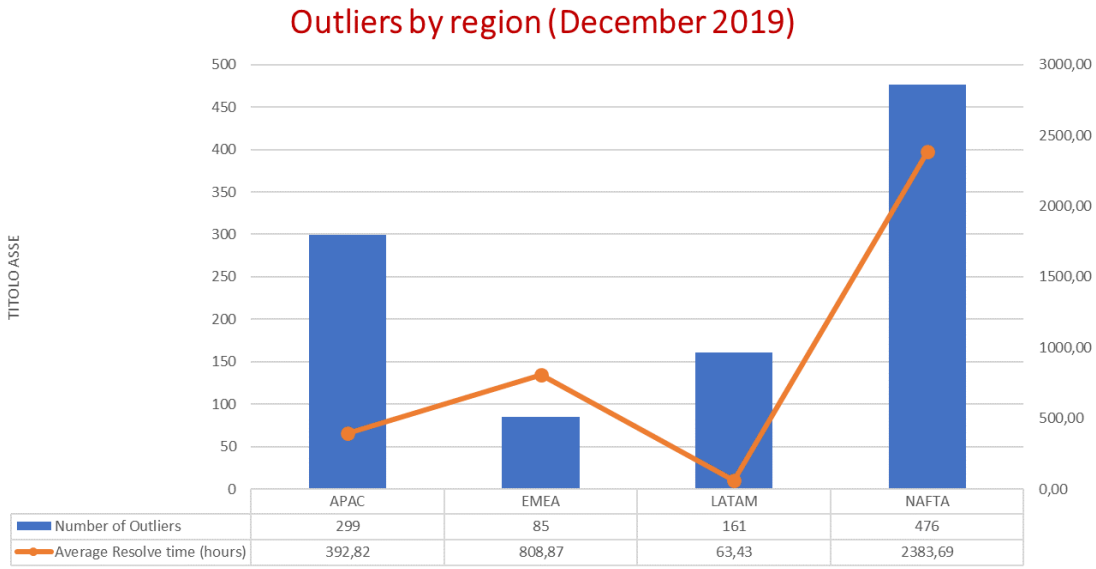
After identifying the relationship between number of reassignments and resolve time, it was necessary to understand how the way each region works affects these indicators. The average resolve time of regions were compared for both samples used in the analysis of data collected in January 2020 about incidents closed on December 2019.



Picture 35 - Average resolve time for each region in each sample (incidents closed on December 2019)

From this chart it is possible to get some impressions and first one is the variation of the NAFTA average from original sample A to the manipulated one B (reduction in almost

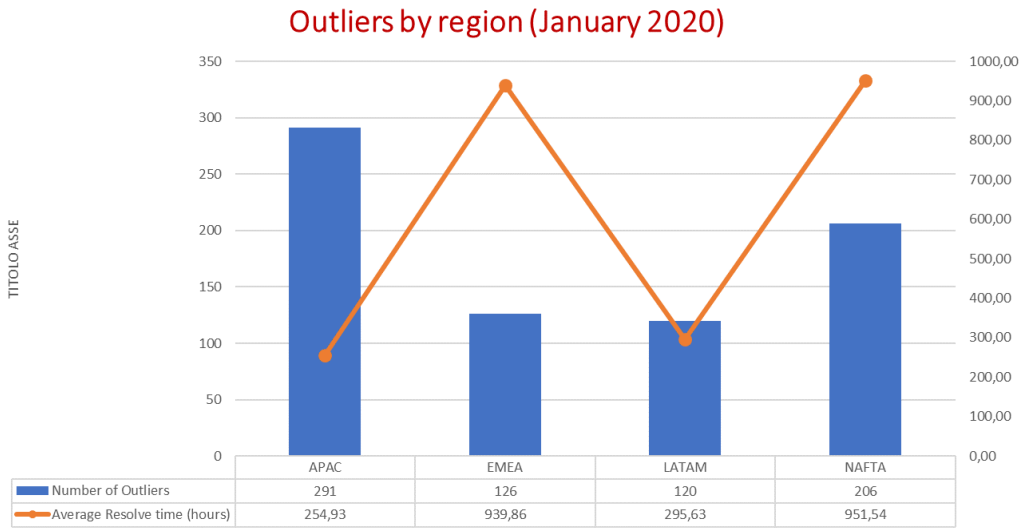
90%). APAC and EMEA had also considerable variations between the samples (reduction in 58 and 33% respectively). LATAM with a variation smaller than 8% was the region less affected by the sample's manipulations and presented the shortest average resolve time in both samples (very close to the APAC score in the second one). These numbers can be used as an indicative of how incidents are being managed among the regions. Having a higher amplitude between the averages of the two samples indicates that regions had bigger quantity of outliers or outliers with longer resolve time. Having more outliers or outliers with longer resolve times indicates that incidents are not being properly logged and managed. From the last chart, the need to drill down on outliers was raised.



Picture 36 - Outliers by region (quantity and average resolve time), data from December 2019

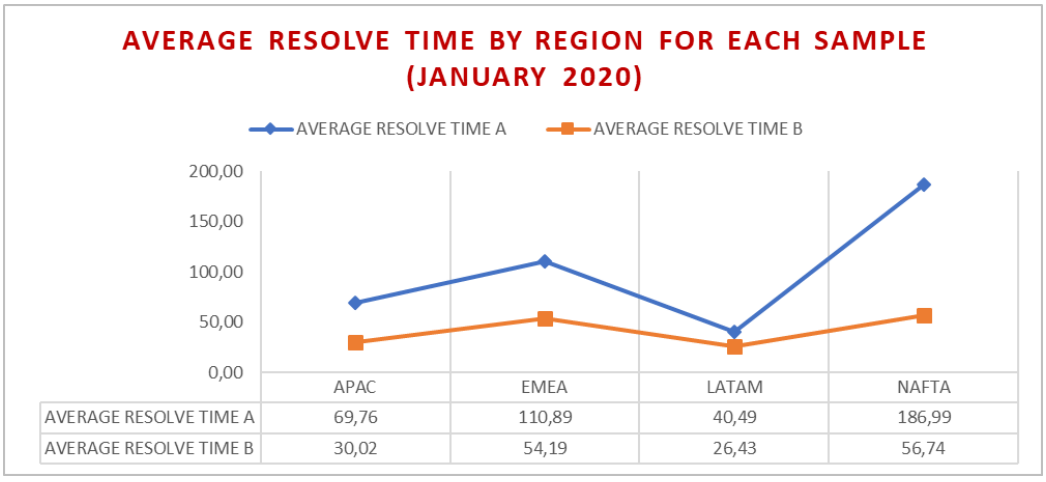
The information that came out from this chart is consistence with what was seen in the previous one. NAFTA has the highest quantity of outliers and an extremely longer average resolve time of outliers than other regions. EMEA is the region with less outliers, but the average of their resolve time is the second highest, being the double of the average from APAC, which is the third longer. LATAM has almost double outliers than EMEA, but a very short average resolve time comparing to other regions. This can be explained by the fact that LATAM was the last region onboarded to Drive IT, having the go-live last year, on January. Thus, it is impossible for LATAM to have incidents open for periods longer than one year, what was observed for other regions. However, this may not be the only reason and these numbers can be used as indicators of the uniformity and consistency of the work in each region.

The number of outliers and the average of their resolve time can vary significantly from a month to another due to many factors. Since all incidents closed on the analyzed month are considered, an activity of cleaning where agents work on aging tickets to clean-up the backlog would increase the outliers. For that reason, same analysis was done for incidents closed on January of 2020.



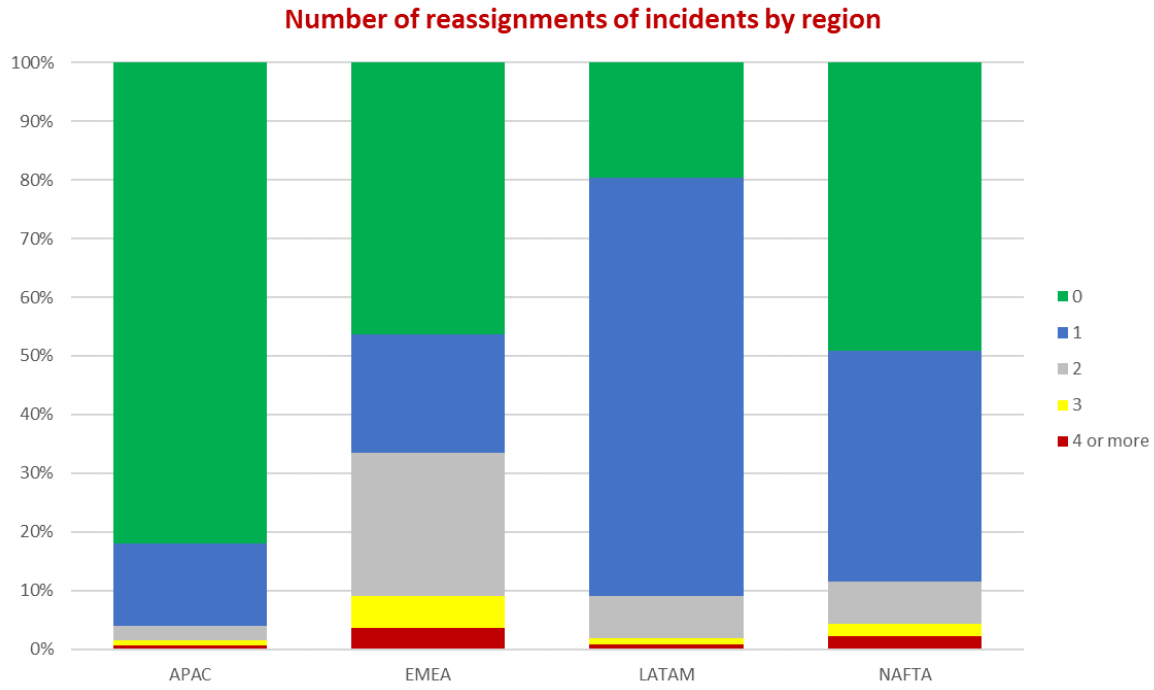
Picture 37 - Outliers by region (quantity and average resolve time), data from January 2020

Again, NAFTA and EMEA showed much longer average resolve time for outliers, what can indicate a gap in the management of aging tickets. With third biggest average resolve time of outliers is LATAM, with an increasing in almost five times regarding the value measured for December 2019. Even so, looking to the average resolve time of the samples analyzed (the original one and the one after removing outliers), it is possible to see that LATAM still presents the shortest value (followed closer by APAC again).



Picture 38 - Average resolve time for each region in each sample (incidents closed on January 2020)

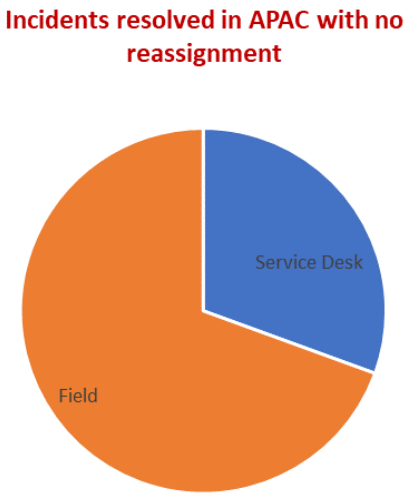
What can explain why LATAM and APAC had best average of resolve time in both months evaluated? To answer this question, the key may be return to the initial purpose of this chapter: evaluate together number of reassignments and time to resolve incidents. The average time to resolve incidents was already presented for each region. For the same period (incidents closed on December 2019 and January 2020) data was collected and analyzed for the number of reassignments of each incident for each region.



Picture 39 - Number of reassignments of incidents by region (incidents closed on December 2019 or January 2020)

Looking to the chart, APAC comes out as the most efficient region to resolve incidents by the initial assignment group, with a rate greater than 80% of incidents resolved without being reassigned. On the opposite way is LATAM with about 80% of the tickets being reassigned at least once before being resolved. However, EMEA deserves attention having a much higher volume of tickets reassigned more than one time, comparing to other regions. Almost one-third of the tickets closed in EMEA from December 2019 to January 2020 were routed between groups two or more times. This may be explained by the existence of the middle layer level of support (the RTS), which is normally engaged before routing a ticket to a field group.

Comparing information observed in that chart with other indicators already seen leads to some questions. How APAC can have most of incidents resolved with no reassignment if the highest volume of their tickets were resolved by field groups, which should work on incidents only after the Service Desk support as level 1? Looking to the chart below, it is possible to see that almost three-fourths of the incidents resolved in APAC by the initial assignment group were resolved by field groups.



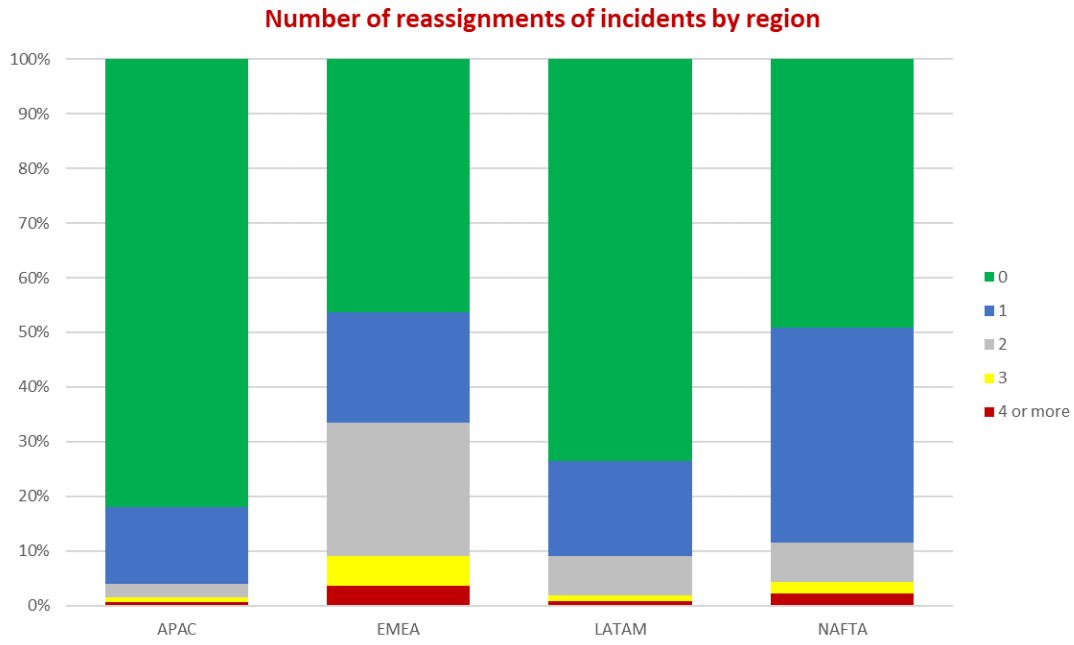
Picture 40 - Incidents resolved in APAC by the initial assignment group (incidents closed from December 2019 to January 2020)

Drilling down on the field groups, it was observed also that 60% of the incidents were closed by the same group: A_IND_ICT_Desktop_Support_AG. This group was also responsible for closing about half of the total incidents closed in APAC during all the analyzed period. How a single field group can be that demanded? Is this a support group for a high concentrated site or a largely used service?

Another question that came out looking to the chart of number of reassignments per region was: How LATAM can have better average time to resolve incidents with 80% of them not being resolved by the initial assignment group? All these information cannot be interpreted alone and there are some concepts that must be understood to be able to do a reasonable evaluation. Even the number of reassignments can have different through the regions. The way EUS model was implemented in Drive IT for LATAM, using routing rules to automatically assign tickets to support groups, had an effect on the initial assignment of incidents created by Service Desk agents.

When an SD agent receives a telephone call, for example, and create an incident on behalf of the affected user, he must fill in some mandatory information before saving the ticket. One of these information is the configuration item, which is used by routing rules to set the initial assignment group. In the support model chosen by APAC, EMEA and NAFTA, the initial assignment group for EUS configuration items are always the Service Desk group itself, thus when the incident is completed with configuration item, the group is not changed.

On the other hand, in the model implemented for LATAM, with field groups as the first support for EUS applications and services, the assignment group of the incident is changed from the SD group to the field (or specialized) group when the configuration item is filled in. For this reason, incidents created by Service Desk agents in LATAM always start with assignment count equals to 1. However, this does not mean that there was support done before by another group. The field group is the initial assignment group to work on the incident that was just created by an SD agent. If we consider that incidents closed by field or specialized groups from Brazil and Argentina, with reassignment count equals to 1 and contact type phone or chat (the available channels to contact the Service Desk there) had, actually, no reassignment, LATAM region has rate of resolution by the initial assignment group close to three-fourths (right after APAC with about 80%).



Picture 41 - Number of reassignments of incidents by region (incidents closed on December 2019 or January 2020, after adjustments on data from LATAM)

Some incidents were individually verified to confirm the scenario of Service Desk just creating and dispatching tickets. This information was confirmed also by the LATAM Incident

Manager. However, this value of incidents resolved by the initial assignment group should be seen as approximated, because there may be some cases where the Service Desk agent do some effort on initial support. Additionally, it was identified that in Argentina there are some cases where the field technician receives calls on his mobile phone and act as a level 1 support, following the same process of Service Desk to create the ticket. But in those cases, normally the reassignment count is equal to zero, because the initial assignment group is already the field group of the technician receiving the call and the incident is generally resolved by the technician himself.

The relationship between number of reassignments and time to resolve an incident was analyzed and it was identified that LATAM region presents the best rates on both indicators. Before, it was already identified that among the four regions of CNHi, LATAM was the one with the most different model of End User Services. But companies are not only looking for faster services. There is a very important point to be considered when taking decisions and choosing between different solutions: cost. How much does it cost the LATAM model? What about the models implemented in the other regions?

6.6 *How much does it cost End User Services in CNHi?*

The contracts made between the companies and suppliers are essential to have satisfactory end user services in terms of quality and cost. Besides the service level agreements (SLAs) that define minimum performance of suppliers, there are other important things to discuss and one of them is the way the services are invoiced. The most common are by fixed cost (a pre-determined fixed amount paid periodically), interactions (received calls, incidents touched, completed tasks, etc.) or availability (minimum technicians by site, Service Desk schedule, etc.). Each format of contract has its advantages and disadvantages and the main ones are listed in the table below:

Table 9 - Advantages and disadvantages of models of EUS contracts

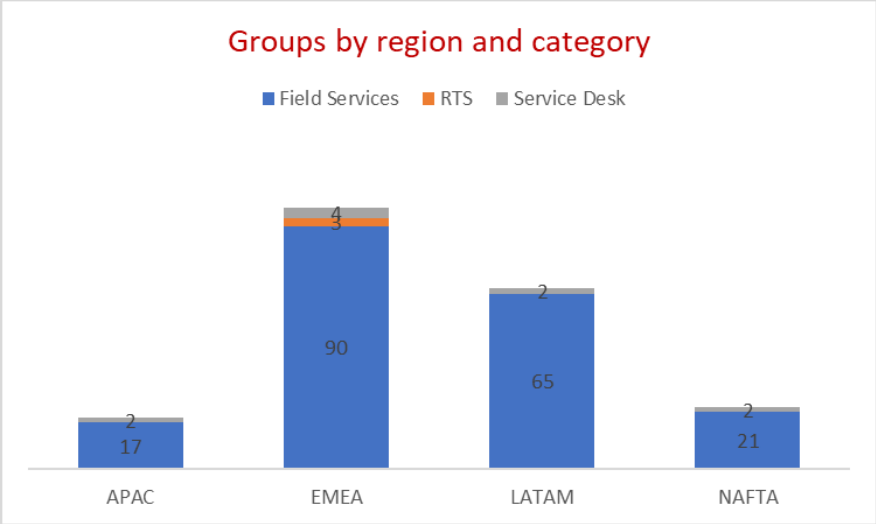
Contract	Advantages	Disadvantages
Fixed price	• Predictability: companies know the cost in advance.	• Inflexible: even in periods of lower demand, cost is the same. In some contracts there are limits when they

	• Power of negotiation: for high demands, services can be cheaper.	are exceeded, renegotiation should be done. • Quality: this kind of contract normally include SLAs that suppliers must respect. But they are not motivated to do more and better.
Interactions	• Flexibility: pays what you consume. Demand for IT services can vary and, when it occurs, company will pay only for what was done.	• Unpredictability: companies cannot know how much they will spend with EUS until receive invoicing. • Complexity to manage: it is more difficult to manage the volume of demand and be sure to be paying for what was really done. Better control systems are required but suppliers can always trick.
Availability	• Effectiveness: resources are normally on site and available to resolve issues faster. • Predictability: known cost as fixed price.	• Cost: this is probably the costly model, due to the need of exclusive dedication of resources. These resources are also often more skilled (and then more expensive).

There are other models of contracts and companies do not need to choose only one (or even a classic one). The most important thing is to make clear and complete contracts between clients and suppliers. It is common also to choose different models for different services, like

it was done by APAC region for Service Desk and Field Services. For the first one, APAC has a fixed price contract based on services and performance agreed. On the other hand, for Field Services, in APAC there either consultants or internal ICT. Fixed price is the most preferred method in CNHi, being applied to all regions. However, to define and review the contract, volume of ticket is considered. In EMEA, for example, there are baselines that if exceeded, contract should be reviewed.

Contract price is normally set according volume of work and resource needed. For this analysis, costs of contracts were not provided and reviewed. The volumes of tickets were already presented and compared. In order to understand how many resources each region uses to deal with their volumes of tickets, a comparison between the EUS groups can be useful.

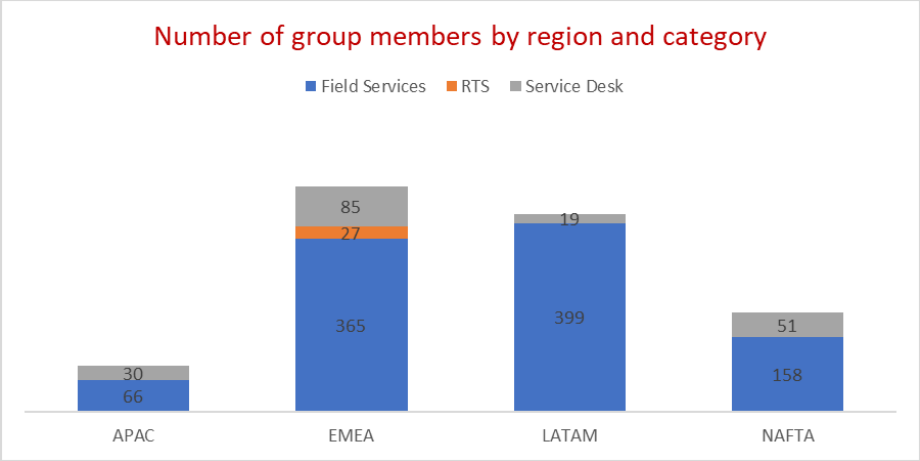


Picture 42 - EUS groups divided in categories among the regions

The model implemented by LATAM, having field services as initial support, demands a bigger quantity of groups that are directly related with the number of locations supported. This is confirmed by the chart above, having LATAM with a high number of groups and being most of them of category Field Services. What maybe was not in line with what was expected is EMEA having even more groups than LATAM and being the region with more groups. It may be explained by a much larger number of locations comparing to other regions. EMEA includes many countries and even if there are centralized and remote support like Service Desk and RTS, local groups are required for need of level 2.

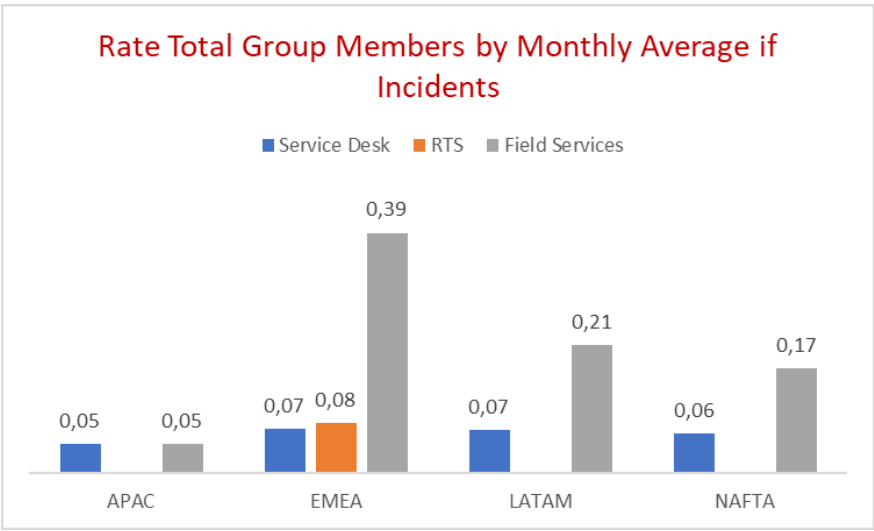
The number of groups can be a good indicator about how the model of service is structured and managed, however, a group can have just one member or a hundred. Thus, it is very important to know how many resources are engaged by each region on EUS activities.

Summing group members it is possible to estimate or have an indicator of this number, because the same person can be member of more than one group. But, since being member of a group means that the resource is part of that scope, it was summed for each category of support and region the total group members.



Picture 43 - Number of group members for each support category in each region

No surprise comparing this chart with the previous one about quantity of groups. EMEA and LATAM have the highest number of groups and members. The proportion of members for each category is also consistent with the share of groups showed before. The information about how many groups and resources alone is not enough to get conclusions. Higher number of groups can be justified, for example, by a higher demand. Thus, it is important to relate this metrics to other ones and, then, get useful information. In order to evaluate the efficiency of the use of resources, it was calculate the rate of group members by average monthly volume of tickets for each region.



Picture 44 - Efficiency using the resources to resolve incidents

This information can be interpreted as how many resources are necessaries to resolve one incident in that region (for each category of support). Thus, as lowest the score, as better it is. APAC had then the best score, with 0,05 for both Service Desk and Field Services. All the other regions had similar score than APAC for Service Desk category, but they differ considerably for Field Services. EMEA presents, by far, the highest score, with more than one-third resource for each resolved incident in one month. It worth to say that EMEA and LATAM have similar number of group members for Field Services (365 and 399 respectively), but LATAM has a much lower rate of resources by resolved incidents due to the higher volume (doble of EMEA) of tickets resolved by Field Services.

7 Conclusions

It was not an objective of this work to conclude what is the best model of End User Support to adopt. The main objective was, through data analysis, investigate how the Incident Process is managed among the regions, provide feedbacks and identify improvement opportunities. One of the most important output from this work was to understand that there are clearly two main approaches adopted that differ in the first level of support. One approach is used by LATAM, where field services' groups are the initial responsible for support, and the other one is used by the other regions and keeps the Service Desk as the first point of contact.

This big difference between LATAM model compared to other regions was identified through results of data analysis together regional Incident Managers and the global Incident Process Manager. Analyzing data it was possible also to confirm the implementation of these approaches and identify some inconsistencies like APAC having a similar rate of incidents being resolved by fields' groups than LATAN, as if they were following same approach. APAC Incident Manager confirmed that Service Desk should be the first and main level of support and has compromised to investigate why this result, especially why a single field group was responsible for closing almost half of their incidents in the analyzed period.

These decision on which approach to use can imply in important aspects like available and preferred channels of contact for end users, efficiency on tickets' resolution and costs. The model applied by LATAM focus on not having a dedicated Service Desk, because there, it does mostly registration and dispatching. However, registration can be done by the end user himself using the portal or using a virtual agent like Ceni Dutra (a customization of Sophie, the smart agent solution provided by Stefanini). Dispatching can be automatically done by the platform Drive IT based on pre-configured routing rules. Thus, the only remaining value added by the Service Desk is the small and simple tasks its agents can perform. But most of these tasks could be performed by the user following documented procedures or having support from a trained virtual agent. Thus, for LATAM, having users calling to the Service Desk is cost that could be avoided and other channels of contact are preferred.

In other regions, the telephone is still the main type of contact, even if in APAC and NAFTA they use considerably email as well. In both types of contact – email or phone -, a Service Desk agent is engaged to take a call in charge. Then, the agent tries to resolve the incident and, if he or she is not able to do it, the ticket is routed to a field services' group. In

the case of EMEA, they added a middle and remote layer to be engaged before routing tickets to field groups in most cases. It was identified, although, that as much as a ticket is reassigned, as longer tends to be its time of resolution. The regions presenting less rates of tickets reassignments were LATAM and APAC. Both regions had also faster average time of resolution of incidents. Again, it is important to highlight that APAC should be revaluated.

Each approach has its associated costs and they differ mostly on the type of contracts and price of resources. Having allocated and dedicated technicians for field services is normally costly. Contracts and their associated costs were not analyzed by this work, but number of groups and their quantity of members were obtained for each region and service category (Service Desk, RTS or Field Services). These data were analyzed together the average volume of incidents closed by each region and category to evaluate how many resources are needed to resolve an incident. APAC appears again with best results, but one of the questions to be answered is why APAC has a volume of tickets so higher. Reminding, APAC, has, by far, the highest rate of incidents by number of active users among the regions. After APAC, NAFTA and LATAM had similar results and EMEA had the highest rate of resources for incidents closed by Field Services' groups.

Another conclusion from this work is that data provided by technicians to Drive IT need to be improved if company wants to use data analysis to get useful and trustable information about tickets. APAC, for example, needs to correctly categorize the type of contact when agents receive phone calls or emails. For all regions, information provided on tickets resolutions must be improved and standardized. General classifications must be avoided and an alignment is necessary between the regions on what use, how and when.

8 Contributions and Future Works

The most important contribution of this work was to understand and document the differences between the four regions of CNHi in the way they implement and manage End User Services. This activity was never done before using data analysis and confronting results with regional EUS leaders. The monthly meeting with them were great opportunities to discuss and discover important points about the process and identify improvement opportunities.

Currently, three of the four regions of CNHi have the same main supplier of EUS services that is Stefanini. Only APAC doesn't have Stefanini in any activity. Having the same supplier globally would be an opportunity to standardize and improve the processes among the regions. This work can be very useful for this subject, providing information, trends and evaluations about different ways to manage EUS.

This work was done only on the Incident Process and future work would be to do a similar analysis on the Service Request Fulfiller Process too. Innumerous service requests are created daily for IT needs and it is important to understand how the regions manage them. After doing an analysis for Service Requests, a final report could be done considering both process and regional peculiarities managing them. Its results could be valuable inputs for staff on decision makings related to End User Services.

Bibliographic References

Barbieri, C. "*Governança de Dados-Parte I-Introdução*". Blog do Barbi-Carlos Barbieri, 2012.

Cao, J.; Diao, X.; Jiang, G.; Du, Y. "Data Lifecycle Process Model and Quality Improving Framework for TDQM Practices". IEEE, 2010.

Conger, S., Winniford, M., & Erickson-Harris, L. (2008) "Service management in operations", Proceedings of 14th Americas Conference on Information Systems, Canada, Toronto. pp. 1-10.

Drive IT Global Services. "Incident Management Process Guide". Fiat Chrysler Automobiles and CNH Industrial, 2015.

Drucker, P. F. "The New Realities". New Brunswick, NJ: Trans. Publishers, 2003.

Flycast Partners. "Understanding the ITIL Service Lifecycle". 2018

Gartner. "Magic Quadrant for IT Service Management Tools". 2014.

Gartner. "Magic Quadrant for IT Service Management Tools". 2019.

Hertvik, J. "ITSM Frameworks: Which Are Most Popular?". Bmc blogs, 2017.

Hoffer, J. A.; Prescott, M.B.; McFadden, F.R. "Modern Database Management, 8. ed. Upper Saddle River, NJ: Pearson Education, 2007.

Iyengar, S. "Analytics for ITSM: 5 Ways to Improve IT Service Delivery". EnterpriseAppsToday.com, 2016.

Knapp, D. "The ITSM Process Design Guide". J. Ross Publishing, 2010.

ManageEngine. "The definitive guide to ITIL incident management". 2019.

Moore, D. S. and McCabe, "G. P. Introduction to the Practice of Statistics", 3rd ed. New York: W. H. Freeman, 1999.

Primark,F. V. Decisões com B.I. (Business Intelligence).1ª ed. Ciência Moderna, 2008.

Rai, A., & Sambamurthy, V. (2006) “Editorial notes-the growth of interest in services management: Opportunities for information systems scholars”, Information Systems Research, 17(4), pp. 327- 331.

Shahsavarani, Narges and Ji, Shaobo, "Research in Information Technology Service Management (ITSM): Theoretical Foundation and Research Topic Perspectives" (2011). CONF-IRM 2011 Proceedings. 30.

Surbhi S. “Difference Between Goods and Services”. Keydifferences.com, 2018.