Extensive analysis with Rabobank event logs

Ziv Hochman (8454434), Stylianos Psara (2140527), Andrikopoulos Panagiotis (1780743), and Ruben van Raaij (8893322)

Team 1, Utrecht University
{z.hochman, s.psara, p.andrikopoulos, r.g.vanraaij}@students.uu.nl

Abstract. In this project, we employ process mining techniques to analyze Rabobank's BPIC 2014 event logs, which include records from the service desk and IT services. Our primary objective is to identify inefficiencies in incident management processes and propose actions to address their root causes. Initially, we conduct a comprehensive analysis of the process model to identify frequent paths and common process flows. Subsequently, we examine incident resolution time based on incident priority levels, reassignment frequency, and the types of assets involved. Furthermore, we analyze re-opened incidents to quantify the time lost in re-resolving previously closed cases. Finally, we evaluate team performance to assess efficiency based on workload and resolution times, identifying teams that demonstrate better in specific tasks. These insights are intended to assist Rabobank in optimizing resource allocation, improving incident management, and enhancing overall service quality.

1 Introduction

Process mining is an emerging field that extracts insightful information from event logs containing millions of traces. Organizations use it to derive valuable insights from their operational data. By leveraging event logs generated by information systems, process mining provides a detailed view of actual business processes, revealing patterns, bottlenecks, and deviations from expected behaviors. Essentially, process mining bridges the gap between model-based process analysis [1] and data-centric process analysis [2] by using real-world data to uncover actual process flows and compare them with theoretical models. This helps organizations validate and refine their process models, gaining valuable information about the dynamics and performance of their operations.

[1] This approach involves creating theoretical models of how processes should ideally work. These models, often developed using domain knowledge, serve as benchmarks to compare against actual process execution [1]

[2] This approach focuses on analyzing the actual data generated by processes to understand how they are truly functioning. It involves examining event logs to identify patterns, bottlenecks, and deviations from theoretical models [1]

This report will analyze the Rabobank event logs from BPIC 2014, which contain detailed service desk and IT services records. Furthermore, this analysis uses process mining to discover inefficiencies and gain a deep understanding of time-consuming incidents and problematic assets, such as frequently re-opened incidents. Our goal is to propose suggestions for these issues, provide valuable insights, and identify the sources of the problems.
The rest of the paper is organized as follows. Section 2 provides an in-depth explanation of the Rabobank event logs used in the analysis. In section 3, we delve into the business questions and detail each question's motivation. Section 4 shows our analysis and findings based on the established procedures. Finally, we conclude in section 5.

2 Data description

Rabobank maintains a comprehensive log of phone calls and emails within their interaction records. The log manager referred to as the Service Desk Agent, can either address the issues directly or escalate them to the designated assignment group, which possesses greater technical expertise. The records encompass interactions, incidents, and changes.

The Interaction record organizes incidents within a single record to streamline the data.

The Incident record provides detailed information about each incident, including its impact, urgency, cause, and status.

The Change record identifies and resolves recurring issues within the system, allowing for service analysis and improvement based on the investigation team's findings.

For the purposes of this analysis, we will focus exclusively on the Incident (activity) record and disregard the Interaction record and the Change record.

By utilizing data from the 4TU Research Data website [3] and the official quick reference of data columns from Rabobank [4], we can construct a detailed data profile of the Incident Record, as shown in Table 1.

Column	Summary	Datatype
Incident ID	Unique ID of an Incident-Record	Object
Activity	Description of the Activity	Object (Categorical)
ActivityTimeStamp	Time of the activity	DateTime
Asset Affected	Application ID that is affected	Object
Asset Type Affected	Application Type	Object (Categorical)
Asset Subtype Affected	Application Subtype	Object (Categorical)
Service Affected	Service ID that is affected	Object
Status	Status Category of the record	Object (Boolean)
Impact	Service disruption level to the customer	Integer
Urgency	Urgency level to the customer	Integer
Priority	Impact + Urgency level to the customer	Integer
Category	The category of the record given the knowledge document	Object (Categorical)
Number of Reassignments	Amount of reassignments before the incident is resolved	Integer
Open Time	Date and time the record was opened	DateTime
Reopen Time	Date and time the record was reopened	DateTime
Resolved Time	Date and time the record was resolved	DateTime
Close Time	Date and time the record was closed	DateTime
Handle Time	Time the record was handled by the agent	Integer
Closure Code	Short code to classify the service disruption	Integer
Asset Caused	Application ID that caused the disruption	Object
Asset Type Caused	Application Type that caused the disruption	Object (Categorical)
Asset SubType Caused	Application SubType that caused the disruption	Object (Categorical)
Service Caused	Service ID that caused the disruption	Object
Assignment Group	The team responsible for this incident activity	Object

Table 1: BPI 2014 Challenge Data Profile

3 Business questions

3.1 Business question 1

What is the average time taken to resolve incidents? Additionally, how does this average time vary based on different priorities, types of assets causing the incidents, and the number of times a case is reassigned?

Motivation: Analyzing resolution times is crucial for identifying delays and inefficiencies. By understanding how resolution times vary among different priorities, Rabobank can allocate resources more effectively, reduce downtime, and ensure that high-priority incidents are resolved quickly, thereby improving customer satisfaction. Additionally, analyzing the types of assets that cause the most time-consuming incidents can help identify problematic assets and target them for improvements. Observing patterns between multiple reassignments and increased resolution times can help Rabobank improve initial assignments and resolve inconsistencies among different assignment groups.

3.2 Business question 2

What percentage of incidents are re-opened after being resolved, and what are the common reasons for re-opening based on the closure code and the asset type

that caused the incident? How many business hours were lost on re-opened incidents?

Motivation: High re-open rates can indicate incomplete or ineffective resolutions. By understanding the reasons behind re-opening, Rabobank can improve its incident resolution procedures and ensure more durable solutions, enhancing customer satisfaction.

3.3 Business question 3

How do different assignment groups perform in terms of resolution times and incident handling efficiency? How does the workload affect them? Are specific teams performing better on specific tasks?

Motivation: Comparing performance across assignment groups helps identify the top-performing teams for high-urgency incidents and those needing improvement. Additionally, this analysis allows us to determine which groups excel in handling specific asset types, facilitating better assignment decisions.

4 Analysis

First, we imported the dataset into Disco and configured the columns as follows: "Incident Id" was set as the case ID, "Activity" as the activity, "ActivityTimeStamp" as the timestamp, and "Assignment Group" as the resource. To efficiently analyze the data and address the business questions, we decided to include only completed cases, focusing on those that went through the entire process cycle.

To understand the desired process flow, we referred to information about "Incident Management" provided by Fluxicon [2]. According to Fluxicon, "After closing the Incident-record, the customer receives an email to inform that the issue is resolved." Therefore, we assumed that a complete case should end with the activity "Mail to Customer." However, using Disco's filtering options based on endpoints, we couldn't find any cases with "Mail to Customer" as a possible endpoint, as there is no case that ends with this activity.

Next, we looked for another endpoint from Fluxicon, which states that "After solving the issue for the customer, the Operator relates the Incident-record to the Configuration Item (CausedBy CI) that caused the service disruption.". We then filtered our data to include only cases ending with the activity "Set asset caused." As shown in Figure 2, this resulted in 19,575 cases (42% of the total 46,601), indicating that these cases, while frequent, are not the norm but rather a common deviation.

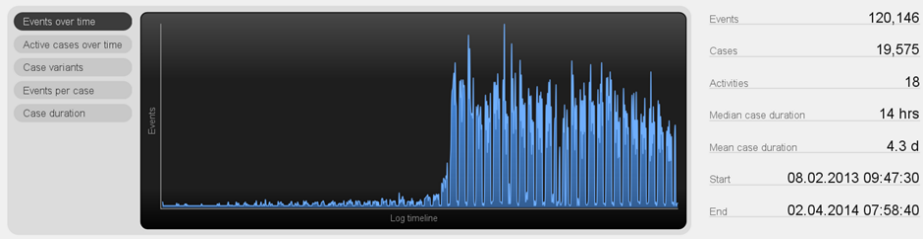

Fig. 2: Disco's Statistics Tab: Overview of Event Log Filtered by Endpoints "Open" and 'Asset Type Caused"

The logical assumption is that a process begins with the activity "Open" and ends with the activity "Close." By applying a filter to keep only the cases that start with "Open" and end with "Close," we confirmed that these cases represent the majority (56% of the total cases). However, from the analysis of the process map (see Figure 3), which shows the most frequent path without any filters, we observe that both "Close" and "Set Asset Caused Type" are part of the frequent path. Additionally, based on the previously mentioned statistics, we can conclude that both "Close" and "Set Asset Caused Type" should be considered as possible endpoint activities.

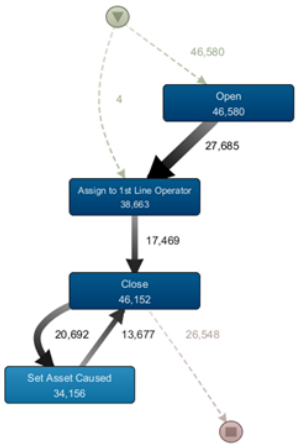

Fig. 3: The most frequent path without any filtering

Therefore, we applied the "Endpoints" filter to include only cases that begin with the activity "Open" and end with either "Close" or "Set Asset Caused." This resulted in the process map shown in Figure 4, with a total of 46,111 cases and 301,886 events.

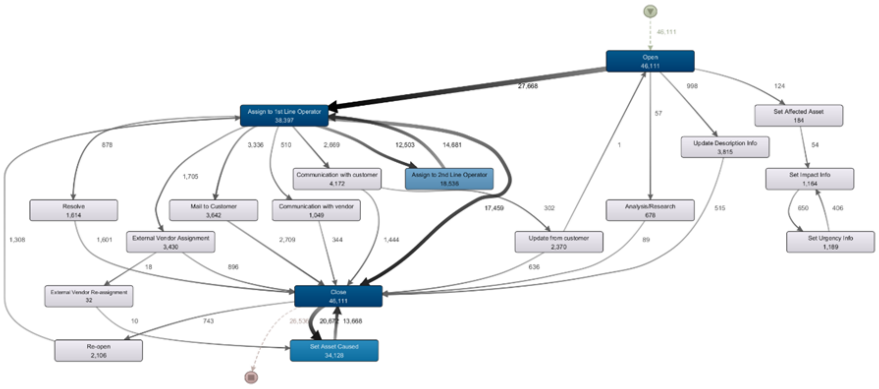

Fig. 4: The final process map, filtered by endpoints 'Open" and 'Close" along with 'Set Asset Caused" activity

4.1 Question 1 Analysis

To address the first business question, we used Disco to observe the mean duration time and then utilized Power BI for further analysis. Specifically, we examined the average resolution time in relation to the incident priority, the type of assets causing the incident, and the number of case reassignments.

First, we observed that the mean duration was 5 days, with the most common path having an average duration of 29 hours. We exported the filtered CSV file from Disco and imported it into Power BI. To analyze the mean duration time, we created a new column named "resolution time," which represents the hours spent between the first open event and the final close event. We defined the resolution time of an incident as the period between its opening and closing phases. Although many incidents concluded with a "Set Assets Caused" activity after closure, we excluded this time from the resolution time calculation.

As shown in Figure 5, there is an expected uptrend in the average resolution time from priority level 2 to priority level 5 (with priority 1 being the highest and priority 5 the lowest). However, we observed an unexpected result: cases with priority level 1 had a higher average resolution time than those with priority levels 2 and 3. Since higher-priority cases should be resolved as quickly as possible, this anomaly suggests that priority level 1 cases might have a higher level of difficulty.

For further clarification on incidents of priority level 1, Rabobank can communicate with Teams 0002, 0171, 0199, and 0203, as these teams are responsible for handling these cases.

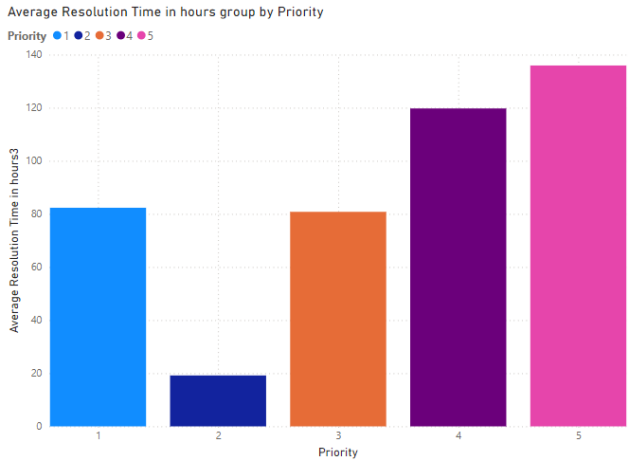

Fig. 5: Average resolution time (in hours) for each priority level

Furthermore, upon analyzing the resolution time concerning the number of reassignments, Figure 6 illustrates that up to 15 reassignments encompass 99.7% of the total cases. Notably, within this range, the resolution time escalates with an increase in the number of reassignments.

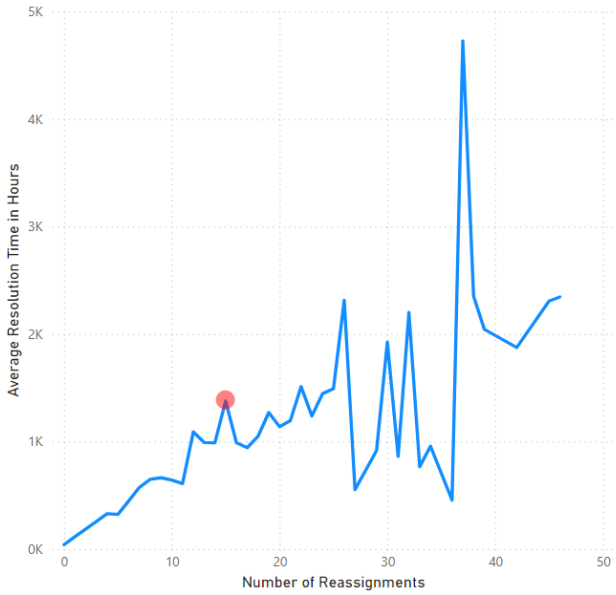

Fig. 6: Average Resolution time (in hours) by number of Reassignments

Moreover, after discovering the proportional correlation between number of reassignments and average resolution time, we delved into which type of assets causing incidents corresponded to the highest average number of reassignments. As depicted in Figure 8, assets with undefined types exhibited both the highest average number of reassignments (7.57) and the longest average resolution time (503 hours). Remarkably, these undefined assets were dispersed across all priority levels. This indicates that when teams were unable to determine the type of asset causing the disruption, the resolution time significantly increased. Therefore, the company should conduct a deeper investigation into these incidents. By preparing teams to better identify and address incidents involving undefined asset types, the company can potentially resolve these cases more quickly in the future. Additionally, our analysis highlights the importance of more accurate initial assignments and better team coordination. By initially selecting the most suitable team for the problem, the company can significantly reduce the need for reassignment later.

In the table below (see figure 7), we present the top ten teams that are frequently involved in tasks with undefined asset causes.

Resource	Count of Case ID
TEAM0015	240
TEAM0008	218
TEAM0002	173
TEAM0003	156
TEAM0024	124
TEAM0016	91
TEAM0017	81
TEAM9999	61
TEAM0014	59
TEAM0207	49

Fig. 7: Enter Caption

(a) Average number of reassignment by asset type caused

(b) Average resolution time (in hours) by asset type caused

Fig. 8: Average number of reassignment and resolution time by asset type caused

4.2 Question 2 Analysis

To address this business question, we used Disco and Power BI. Initially, we applied the **"endpoints"** filter in Disco to the data as previously described. Additionally, we applied the **"Follower"** filter because we were specifically interested in incidents that were re-opened after being closed or resolved. This filter allowed us to retrieve all of these incidents.

After applying the "endpoints" filter, we retained approximately 98% of the total cases. However, after adding the "Follower" filter, this number was reduced rapidly down to 4% of the cases, as illustrated in *Figure* 9, which shows the final process map after applying both filters.

This analysis will help the business gain insights into the reasons behind reopened incidents and understand how these incidents impact operations, particularly in terms of the loss of time that could have been spent addressing new incidents.

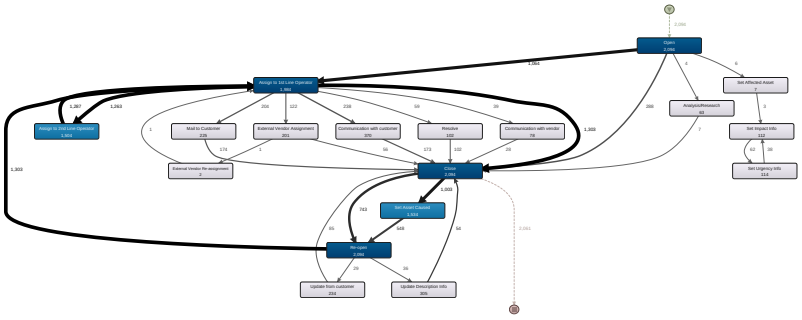

Fig. 9: The complete process map after applying the filters

Since only 4% of the total cases were re-opened, we can conclude that most teams handle incidents effectively and efficiently without the need for re-opening. However, the 2,094 re-opened incidents require further analysis. To facilitate this, we calculated the average time lost due to these incidents to motivate the need for further investigation. This deeper analysis will help identify the causes of re-opened incidents and develop strategies to minimize their impact, ensuring more streamlined operations and better resource allocation.

To calculate the desired average, we needed to create a few intermediate columns. First, we created a column called **"FirstCloseOrResolveTimestamp"** to calculate the initial "Close" or "Resolve" timestamp for each incident. This helps us exclude any time an incident was re-opened before it was closed, as these incidents do not match the focus of our analysis. Next, we added a column named **"PreviousReopenTimestamp,"**, which records the most recent time the incident was re-opened for each activity. This ensures accurate calculation of the time differences between the close and re-open timestamps by considering only the time spent between each re-open and the corresponding close activity(as from close to re-open, the incident is considered inactive). Then, we created the column '**"TimeDifference"** to compute the duration between the current "Close" activity and the previous "Re-open" timestamp. For each "Close" activity (except the first appearance), it calculates the difference between the "Close" timestamp and the **"PreviousReopenTimestamp."** Finally, we introduced a column titled "AccumulatedTime" to aggregate the total hours lost for each incident throughout its cycle(as an incident can have multiple closes and re-openings), using the values from the **"TimeDifference"** column.

After following this process, we obtained the results shown in Figure 10:

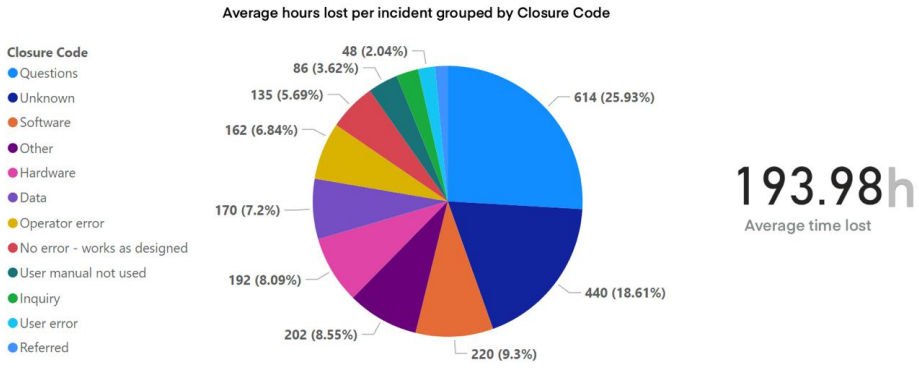

Fig. 10: Average hours lost per incident grouped by Closure Code, with the average hours lost shown on the right.

As indicated by the data in Figure 10, the average time lost due to re-opening an incident after its resolution or closure amounts to 193.98 hours, which equates to approximately 8 additional days per incident. This prolongs the resolution of older incidents and can potentially hinder the timely handling of new incidents by consuming resources. Our analysis reveals two unique findings. Firstly, incidents categorized as "Questions" in the "Closure Code" that were re-opened have the longest average resolution time, losing 614 hours per incident on average until the final close. This suggests a potential issue with either documentation or customer explanations provided by the teams. Investigating these incidents will help the company mitigate and possibly reduce the time lost in handling such incidents. Secondly, incidents classified as "unknown" require an average of 440 hours to close re-opened incidents. Further analysis is required to gain deeper insights into these incidents.

We began by investigating the assets identified as the cause of these incidents with "unknown" "Closure Code" as seen in figure 11.

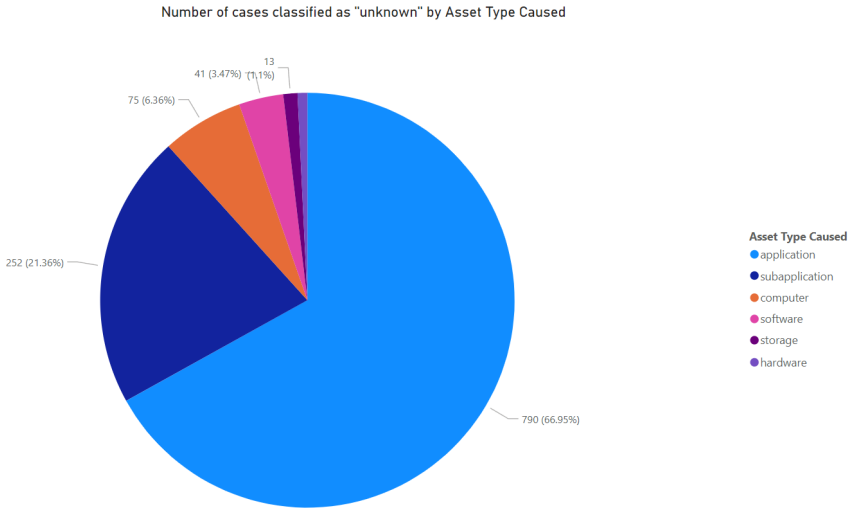

Fig. 11: Count of "unknown" incidents grouped by "Asset Type Caused"

As shown in Figure 11, the asset category responsible for the highest number of "unknown" incidents being re-opened was "application", accounting for 720 incidents. Therefore, it is crucial for the company to investigate these incidents with domain experts in application management to identify and address underlying issues, aiming to reduce the recurrence of incident re-openings.

4.3 Question 3 Analysis

This business question aimed to evaluate the performance of different assignment groups, referred to as "Resources"[3], focusing on their resolution times, incident handling efficiency, and expertise in specific and different asset types. To achieve this, we employed Python for data analysis, assuming that the teams represented in the logs are responsible for solving the incidents and consist of approximately the same number of members, ensuring a fair comparison.

Incident handling efficiency was quantified using resolution hours, defined as the difference between the incident close time and open time. The dataset was grouped by assignment group/resource, and key metrics such as resolution time and case count were aggregated. Specifically, if R denotes the set of all resources, and T_i represents the resolution time for case i, the analysis enabled us to identify performance disparities among the groups. The approach provided insights into whether specific teams excelled in handling particular types of tasks more efficiently, which is calculated in equation 1.

$$\text{Avg Resolution Time}_R = \frac{1}{N_R} \sum_{i=1}^{N_R} T_i \tag{1}$$

Where:

- N_R is the total number of cases handled by resource R.
- T_i is the resolution time for case i handled by resource R.

By filtering the top seven teams with the highest case count or average resolution time, we generated Figure 12, which presents these metrics in a bar plot. The cyan part shows the Average Resolution time, the yellow part shows the number of Cases/Incidents, and the green shows the overlap between these two.

The analysis of this figure revealed that TEAM0008 handled a large volume of cases/incidents while maintaining a low average resolution time, making TEAM 0008 a high-performing team. Conversely, TEAM0004 and TEAM0027 exhibited high-resolution times coupled with a low number of cases, making them a low-performing team. Furthermore, upon closer examination, TEAM0007 and TEAM0031 exhibit nearly identical case counts. However, TEAM0031 resolves incidents in almost half the time of TEAM0007. This discrepancy might suggest that TEAM0007 faces more challenging incidents or experiences slower resolution times due to bad performance. Similarly, TEAM0016 and TEAM0191 manage nearly the same number of cases, yet TEAM0191 resolves incidents in almost one-third of the time taken by TEAM0016. Finally, TEAM0105 achieves the

[3] The manager of each Resource assigns the incident to either a first-line operator, a second-line operator (who has more expertise), or an external operator. The teams, referred to as Resources within the dataset, are responsible for solving the incidents.

shortest resolution times, which is almost imperceptible in Figure 12; however, handling very few cases compared to others.

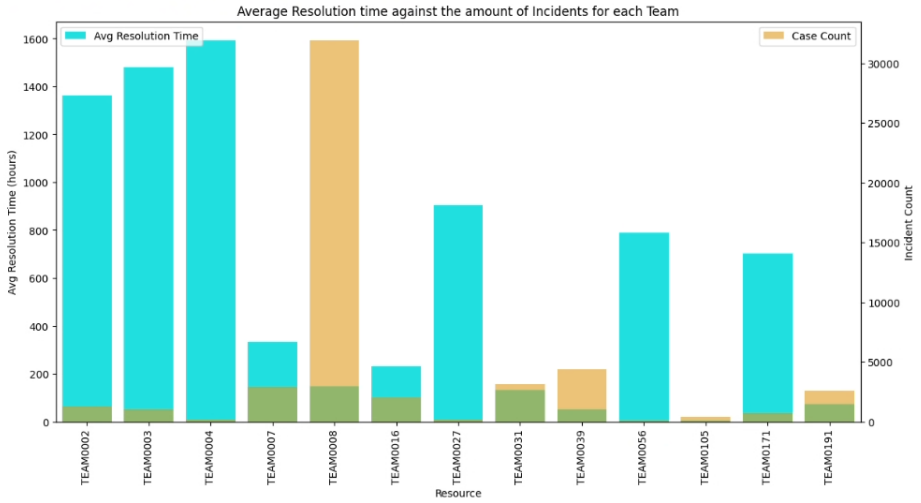

Fig. 12: Average Resolution Time (Cyan colored) against the amount of Incidents (Orange colored) with their overlap (Green colored) for each Team/Resource

You might conclude that TEAM0008 has the best performance; however, the Asset type might have a great influence on the resolution time as seen in Figure 15, so to prove that TEAM0008 has the best performance, we need to further analyze the performance of the teams using another metric such as their percentage of cases per asset type. This bar plot shows the Average Resolution time for each Asset Type with an error bar indicating the variability around the central tendency measure.

To gain deeper insights into team performance across specific tasks and identify time-intensive processes, we developed two figures illustrating the distribution of cases handled by each team. Figure 13 highlights teams with lower performance metrics, while Figure 14 showcases teams demonstrating higher performance. These visualizations provide clarity on which teams excel in particular tasks and illuminate which tasks may require more time-intensive efforts. Each table has its Column name abbreviated to its first 3 letters.

Analysis of Figure 14 reveals that asset types such as **Phone**, **Application Component**, **Display**, **Hardware**, and **Network** are less frequently selected. Figure 15 indicates that the black error bar is absent for the **Phone** asset type, suggesting that it is probably associated with only one case (indeed, it is only one case that we observed from the data)handled by TEAM0008. This observation implies that TEAM0008 also specializes in rare incidents, which maybe an indicator that has good expertise in multiple areas/
Furthermore, TEAM0007 and TEAM0016 exhibit strong performance in handling **Application** incidents. TEAM0105 shows proficiency in resolving **Software** type incidents while also managing incidents with low-resolution times. Similarly, TEAM0031, TEAM0039 and TEAM0191 excel with **Application** and **Sub Application** asset type incidents.

Analysis of Figure 13 indicates that **Application**, and **Subapplication** are the most commonly reported asset types for incidents. However, examining Figure 15 reveals that both **Application** and **Subapplication** have very low average resolution times and error bars, suggesting that teams with the highest resolution times are likely dealing with unclustered incidents or other incidents which may cause a high-resolution time as seen in figure 13.

Resource	#N/B	Phon	appl	app.comp	comp	data	disp	hard	netw	offi	soft	stor	suba
TEAM0002	13.328197	0.0	61.093991	0.000000	1.771957	0.077042	0.0	0.000000	0.000000	0.0	0.154083	0.308166	23.266564
TEAM0003	15.145631	0.0	54.271845	0.000000	1.844660	0.097087	0.0	0.388350	0.000000	0.0	0.194175	0.097087	27.961165
TEAM0004	13.407821	0.0	48.603352	0.000000	2.234637	0.000000	0.0	0.558659	0.000000	0.0	0.558659	0.558659	34.078212
TEAM0027	22.602740	0.0	73.287671	0.000000	0.000000	0.000000	0.0	0.000000	0.000000	0.0	2.739726	0.000000	1.369863
TEAM0056	6.299213	0.0	72.440945	1.574803	4.724409	0.000000	0.0	0.787402	1.574803	0.0	1.574803	0.787402	10.236220
TEAM0171	6.022409	0.0	56.302521	0.140056	0.420168	0.000000	0.0	0.000000	0.000000	0.0	0.420168	0.560224	36.134454

Fig. 13: Percentage of Cases per Asset Type per (low performing) Team

Resource	#N/B	Phon	appl	app.comp	comp	data	disp	hard	netw	offi	soft	stor	suba
TEAM0007	0.103341	0.000000	79.090596	0.000000	0.206683	0.034447	0.000000	0.000000	0.000000	0.000000	0.034447	0.034447	20.496039
TEAM0008	0.683664	0.003136	61.482736	0.003136	9.417631	0.526860	0.504908	0.567629	0.514316	0.307335	5.644934	0.802835	19.540879
TEAM0016	4.462972	0.000000	70.279549	0.000000	0.294262	0.000000	0.000000	0.000000	0.000000	0.000000	1.814615	22.903384	0.245218
TEAM0031	0.158831	0.000000	54.606099	0.000000	0.222363	0.031766	0.000000	0.000000	0.000000	0.127065	0.158831	0.095299	44.599746
TEAM0039	0.022889	0.000000	60.723278	0.000000	0.137331	0.000000	0.000000	0.000000	0.000000	0.000000	0.022889	0.045777	39.047837
TEAM0105	0.000000	0.000000	11.448598	0.000000	0.000000	0.000000	0.000000	0.233645	0.000000	0.000000	88.317757	0.000000	0.000000
TEAM0191	0.038986	0.000000	61.793372	0.000000	0.233918	0.000000	0.000000	0.000000	0.000000	0.077973	0.077973	0.038986	37.738791

Fig. 14: Percentage of Cases per Asset Type per (high performing) Team

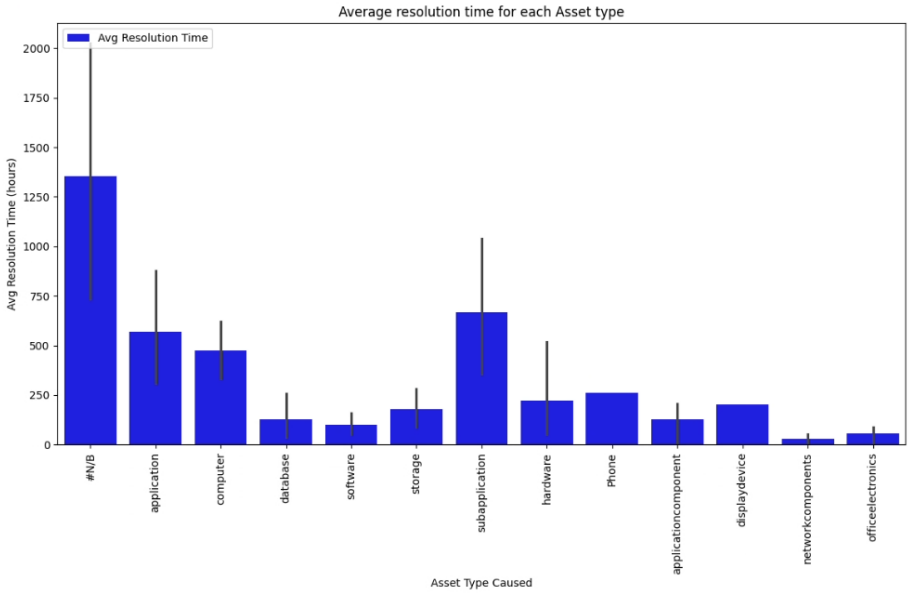

Fig. 15: Average Resolution Time & its Error bar indicating the variability around the central tendency measure per Asset Type

As shown in the figures, the performance of the teams depends on the incident types they got/took:

- TEAM0008 has been involved in most uncommon cases, indicating that it may efficiently handle rare incidents.
- TEAM0007 has many of their incidents in the Application and Subapplication type, making them generally well-performing within this area.
- TEAM0016 also has a lot of Application type incidents but also some in Storage, meaning they are well-performing especially in the storage-type incidents
- TEAM0031 & TEAM0039 & TEAM0191 have great knowledge in both the Application and Subapplication area.
- TEAM0105 works best on Incidents within the Software area.

5 Conclusion

This extensive analysis of Rabobank's event logs from BPIC 2014 has provided valuable insights into the service desk and IT services processes. By applying process mining techniques, we have uncovered patterns, bottlenecks, and deviations from expected behaviors that can significantly impact the bank's operational efficiency and customer satisfaction.

Our findings indicate that the resolution time of incidents varies considerably based on priority levels, with unexpectedly longer times for priority 1 incidents. This suggests that while these cases may be more complex, there may be a need for further investigation from the bank. Additionally, the analysis of reassignments has shown a clear correlation with increased resolution times, highlighting the need for more accurate initial assignments and better coordination among teams.

The investigation into re-opened incidents has revealed that certain closure codes, such as "Questions" and "unknown," are particularly problematic, leading to substantial time losses. This points to potential issues in the resolution process, including incomplete documentation, inadequate communication with customers, and insufficient specialization in the "application" Asset type, as "unknown" closure codes were correlated with many assets of the type application. Addressing these areas could reduce the frequency of incident re-openings and the associated waste of resources.

Performance analysis across different assignment groups has demonstrated that teams vary in their efficiency, with some excelling in handling specific types of assets. This information can be leveraged to optimize the assignment of incidents and improve overall service delivery.

In conclusion, this study has identified several areas for improvement within Rabobank's incident management processes. By implementing the suggested recommendations, such as refining resource allocation, improving initial incident assignment accuracy, enhancing documentation and communication practices, and leveraging team specializations, Rabobank can enhance its operational performance, reduce incident resolution times, and improve customer service outcomes.

References

[1] Wil van der Aalst. *Process Mining: Data Science in Action*. Springer, 2016. ISBN: 978-3-662-49850-7. DOI: 10.1007/978-3-662-49851-4.

[2] Wil van der Aalst. *Process Mining: Data Science in Action*. Springer, 2016. ISBN: 978-3-662-49850-7. DOI: 10.1007/978-3-662-49851-4.

[3] "BPI Challenge 2014 Data Collection". In: *https://data.4tu.nl/collections/*/5065469/1 ().

[4] *Quick reference BPI Challenge 2014*. Tech. rep. TU EINDHOVEN.