Evaluation and Mitigation of Android Application in PT. Aku Pintar Indonesia

Lutvianto Pebri Handoko¹ and Mokh. Suef¹

Abstract—Aku Pintar Indonesia enterprise is one of the educational start-up industries currently developing an Android-based system. System errors could appear in various both the features and administrative processes. The system repair priority could be given to the easiest system error first without taking into account the risk that would arise. The company needed to change its risk management by providing the priority of system repair and considering the effects and frequency of the occurrences. This research aims to help Aku Pintar Indonesia enterprise in choosing the priority of system error repair in order to improve their services to their users. This research used FMEA which allows the risk level of each error modes being assessed. System errors and its frequency were identified by web-based Google Play Console. The disadvantage level appeared from each errors determined by utilizing expert judgment in a Focus Group Discussion (FGD). The risk level of each system errors determined by the frequency of each and the level of the disadvantages, then measure the value of the Risk Priority Number by multiplying the results of severity and occurrence so that the risk value is obtained. The next process of risk mapping based on the risk level uses a modification of the risk mapping table to obtain the error rate for making priority improvements. This research produced a complete document that contains the information needed to plan and prevent repetitive errors, and can reduce the initial system error rate by 4% to 2.4% according to reports from the Google Play Console system.

Keywords—FMEA, System Errors, Risk Management, Application System, Android.

I. INTRODUCTION

One of the things influenced to the developing of android application is system errors or bug that affects any application errors. According to [1], computer system or program failure is caused by the errors that occurs and experts said that was debugging process. “Bug” name came from a small insect that caused damage in Harvard Mark II’s computer in relay part at the time. System error often leads to an application or system that requires bug-fix. That is a challenge for PT. Aku Indonesia which has 269,353 total users to get the least system error / bug. The problems of system error /bug in Aku Pintar application often happened in administrative and application features. According to Google Play Console report, the total of system errors / bugs in Aku Pintar application from 12 March 2019 to 11 May 2019 reached 6,380 bug. Based on the survey data in Google Play Console (22 April 2019), as many as 96.3% of users were free from system errors (bugs) whereas, 3.7% - 4% of users experienced the bugs. The higher number of users is the more of them experienced system errors / bugs. A total of 6,380 cases have occurred over the past three months and PT. Aku Pintar Indonesia need to manage bugfix in order to reduce the disadvantage that caused the distraction in learning processes, reduction in users’ trust, and decreases of users’ convenience, as well as the occurrences of uninstalling that reached 31,360 in total. Therefore, it is necessary to conduct mitigation of risk in system error / bugs by using Failure Mode and Analysis method, so the improvement plan could be run effectively.

II. LITERATURE REVIEW

A. Failure Mode and Analysis (FMEA)

Failure Mode and Effect Analysis (FMEA) is a paradigm/logic, structural analysis of systems, subsystems, device, or processes. Functional magnetism is an analysis of commonly used reliability and security systems. FMEA is one of the methods in reliability and security system that is commonly used. FMEA is useful for identifying the possibility, the cause and consequences of failure mode. A good and accurate identification process could increase the overall reliability and security of a product. On the other hand, there are many purposes for using FMEA, such as identifying and preventing safety hazard, minimizing the disadvantages of product performance decreases and losses, increasing the validation and verification, improving the quality of the processes, being a consideration in product design and manufacture processes, identifying the significance and characteristic of the product, designing preventive maintenance plan and designing an online diagnostic technique [2]. While using FMEA method, it is necessary to understand the component of FMEA, they are Severity, Occurrence, Detection, and Risk Priority Number (RPN). Severity is an indicator that reflects on how significant the effect of a failure mode occurrence. Severity is determined without looking at other indicators, such as Occurrence and Detection, hence, only reviewed the description of failure and the effect of it if happen [3]. Besides that method and formulation explained before, many companies often use alternative method for prioritizing the failure, one of them is by using Severity and Occurrence as the input in
conducting Criticality Analysis, which usually called as Failure mode method, Effects, and Criticality Analysis (FMEA). Because this method does not use the Detection indicator, it needs to conduct supplementary analysis to replace the inability of failure mode detection and its causes [2]. In addition, there are many advantages in using the FMEA method, such as, this method helps system designer to identify and eliminate or control the failure mode that potentially dangerous, decrease the damage experienced by users and system at a time. Through this method, it is able to increase the estimation accuracy of failure possibility that will happen, especially if the data processed by using Failure Mode and Effect Critical Analysis (FMECA).

Lari Nasim [4] conducted a research using FMEA method and the object of the study was the security of the information system technology in an airport. The research had been done by the author using fishbone diagram analysis aimed to analyze the interference that damage the information system in airport and measure the repair priority as well as the mitigation using FMEA, so the maintenance is necessary. According to [5], maintenance could extend life of the product and service.

B. PT. Aku Pintar Indonesia

PT. Aku Pintar Indonesia is a private company engaged in information technology in education started by mapping the interest and talent until guiding in choosing a success career path which fit their interest and talent of Indonesia students.

III. METHOD

In this chapter, the Occurrence and Severity of system errors/bugs in both administrative and features in Aku Pintar application is explained. The occurrence used the frequency of system errors occurrence and the Severity used the potential failure causes.

Occurrence is the frequency of system errors/bugs occurrence which the risk level measurement used the scale “A” for “Very low”, “B” for “Low”, “C” for “Moderate”, “D” for “High” and “E” for Very high” as written in Table 1. The use of this scale is the result of brainstorming with the experts in Android Mobile Developer division of PT. Aku Pintar Indonesia. Similarly, the measurement criteria for Severity as shown in table 2 are the result of brainstorming with experts in the Android Mobile Developer division of PT. Aku Pintar Indonesia.

IV. RESULT AND DISCUSSION

A. Analysis of System Error/Bugs in Administration of Aku Pintar Application

In the discussion and evaluation of the risk mapping of system errors/bugs in the administration section, it is useful to map how severe the effects of this system error are. This will help Aku Pintar Mobile Developer team to prioritize system improvements by reviewing the risk level. The following is the table that explains about Failure Mode Effect Analysis in Administration section of Aku Pintar application.

From the results of the discussion, it was found that the Verification Registration section occupied the level of risk ‘Very High’ due to the occurrence of a force close on the main part of the application that served as the user entry path which caused trouble to users entering or registering to the application and occurs 347 times, made it very dangerous and entered the Very High category, so that happened to other failures as well as what happened in administration section. The Manual Verification was in the risk level “Low” because no force close and not in the main part of application administration and only as an alternative if a system verification failure occurred automatically.

| TABLE 1. OCCURRENCE RANK CRITERIA |
|------------------------------------|
| Risk Level | Level Description | Frequency of Interference | Qualitative Description |
| E | Very high | >500 times | Frequent |
| D | High | 250 – 500 times | Reasonably probable |
| C | Moderate | 150 – 250 times | Occasional |
| B | Low | 50 – 150 times | Remote |
| A | Very low | <50 times | Extremely unlikely |

| TABLE 2. SEVERITY RANK CRITERIA |
|---------------------------------|
| Risk Level | Level Description | Frequency of interference | Qualitative Description |
| E | Very high | There was force close in main section | Hazardous |
| D | High | There was force close in medium section | Significant |
| C | Moderate | There was force close in minor section | Medium |
| B | Low | There was no force close and user started to feel irritated | Minor |
| A | Very low | There was no force close and user did not feel irritated | Insignificant |
Figure 1. Display of the Google Play Console Aku Pintar Dashboard

New Edit Profile occupied 'Moderate' risk level due to a force close but not in the main administration and the incident was only 44 times so that it was in the severity level 1. Get Value Resources occupied 'Low' risk level because there was no force close and not in the main part and the incidence rate was quite low, 47 times. New Profile occupied the 'Moderate' risk level because of the force close but not in the main part of the administration process and the low incidence rate of 16 times. Base Service occupied 'Low' risk level because there was no force close, but the user began to feel small interference and the low rate that was 5 times.

After conducting assessment using Excel, it was found the Administrative Risk Mapping of Aku Pintar application as shown in Figure 1. Risk mapping was made in a 5x5 matrix, adjusting to the measurement criteria of severity and occurrence. The risk mapping can be used to determine priorities. This priority was obtained from the results of the impact level or the severity and processed occurrence level. Divided into 4 risk levels namely 'Very High', 'High', 'Moderate', and 'Low'. There was 1 risk with Very High level of risk. Priority I was the Register Verification. Priority II was the Main Menu. Priority III was New Edit Profile, New Profile and No location Available. Priority IV was Service Phone Receiver and Manual Verification. Priority V was Get Value Resources and Base Service.
### Table 3.
**Analysis of System Error / Bugs in Administration of Aku Pintar Application**

| ID | Risk Description                        | Frequency | Impacted Users | OMG | Severity | Occurrence | Risk Level | Risk Mitigation Details                                      |
|----|----------------------------------------|-----------|----------------|-----|----------|------------|------------|-------------------------------------------------------------|
| 1  | Register Verification                   | 347       | 292            | YES | 5        | 4          | VERY HIGH  | a. Making other registration options (SMS, Email and Whatsapp)  |
|    |                                        |           |                |     |          |            |            | b. Socialization of procedures for registering to users         |
| 2  | No location available                   | 172       | 41             | NO  | 1        | 3          | LOW        | a. Re-check each source code                                   |
|    |                                        |           |                |     |          |            |            | b. Socialize cellphone file access agreement                   |
| 3  | Main menu                              | 254       | 242            | NO  | 1        | 4          | LOW        | a. Re-check each source code                                   |
| 4  | Manual Verification                     | 118       | 18             | NO  | 1        | 2          | LOW        | a. Re-check each source code                                   |
| 5  | New Edit Profile                       | 44        | 33             | YES | 3        | 1          | MEDIUM     | a. Re-check each source code                                   |
|    |                                        |           |                |     |          |            |            | b. Aligning databases                                          |
| 6  | Resources Get Value                    | 47        | 21             | NO  | 1        | 1          | LOW        | a. Re-check each source code                                   |
|    |                                        |           |                |     |          |            |            | b. Aligning databases                                          |
| 7  | New Profile                            | 16        | 8              | YES | 3        | 1          | MEDIUM     | a. Re-check each source code                                   |
|    |                                        |           |                |     |          |            |            | b. Aligning databases                                          |
|    |                                        |           |                |     |          |            |            | c. Routine database repair and cleaning old files              |
| 8  | Base Service                           | 8         | 4              | NO  | 1        | 1          | LOW        | a. Give suggestions (notifications) to users to stabilize the network |
| 9  | Service Phone Receiver                 | 5         | 3              | NO  | 2        | 1          | LOW        | a. Re-check each source code                                   |
|    |                                        |           |                |     |          |            |            | b. Socialize cellphone file access agreement                   |

![Administrative Risk Mapping](image-url)

**Figure 2.** Administrative Risk Mapping
B. Analysis of System Error/Bugs in Features of Aku Pintar Application

In the discussion and evaluation of the risk mapping of system errors/bugs in the Features section, it was useful to map how severe the effects of the system error are. This will help Mobile Developer team of Aku Pintar application to prioritize system improvements by reviewing the risk level. The following table explained about Failure Mode Effect Analysis in Features of Aku Pintar application.

| ID | Risk Description                  | Frequency | Impacted Users | Force CLOSE | Severity | Occurrence | Risk Level | Risk Mitigation                                                                 |
|----|-----------------------------------|-----------|----------------|-------------|----------|------------|------------|---------------------------------------------------------------------------------|
| 1  | Feed                              | 1181      | 567            | YES         | 3        | 5          | HIGH       | a. Re-check each source code  
b. Quality Control of posted articles  
c. Give suggestions (notification) to users to stabilizing the network          |
| 2  | Banding Program Studi             | 935       | 468            | YES         | 3        | 5          | HIGH       | a. Re-check each major's content  
b. Socialize to Campus PIC to regularly update majors                             |
| 3  | Pembahasan Tes Penjurusan         | 235       | 211            | YES         | 4        | 3          | HIGH       | a. Re-check each source code  
b. Give suggestions (notification) to users to stabilizing the network         |
| 4  | Pembahasan Tes Pintar             | 315       | 259            | NO          | 1        | 4          | LOW        | a. Re-check each source code  
b. Give suggestions (notification) to users to stabilizing the network         |
| 5  | Pin point (belajar pintar)        | 240       | 226            | NO          | 1        | 3          | LOW        | a. Give suggestions (notification) to users to stabilizing the network          |
| 6  | Latihan Soal                      | 245       | 224            | NO          | 1        | 3          | LOW        | a. Install a backup server or replacement                                        |
| 7  | Alive open chat                   | 178       | 140            | NO          | 2        | 3          | MEDIUM     | a. Install a backup server or replacement                                        |
| 8  | Overview universitas              | 108       | 102            | NO          | 1        | 2          | LOW        | a. Re-check each source code                                                    |
| 9  | Mengerjakan Tes Pintar            | 148       | 128            | NO          | 1        | 2          | LOW        | a. Re-check each source code                                                    |
| 10 | Detail Universitas                | 84        | 72             | NO          | 1        | 2          | LOW        | a. Re-check each source code                                                    |
| 11 | Endless Recyler View Scroll Listen| 115       | 104            | YES         | 3        | 2          | MEDIUM     | a. Socialize the manual to users                                                 |
| 12 | Pembahasan Minat Bakat            | 146       | 139            | NO          | 1        | 2          | LOW        | a. Re-check each source code                                                    |
| 13 | Soal Minat Bakat DISC             | 82        | 73             | YES         | 5        | 2          | VERY HIGH | a. Re-check every question and its completeness                                  |
| 14 | List Kerja Tes Adapter            | 123       | 103            | NO          | 1        | 2          | LOW        | a. Re-check each source code                                                    |
| 15 | New University                    | 184       | 140            | NO          | 2        | 3          | MEDIUM     | a. Make some server improvements                                                 |
| 16 | Biaya Jurusan                     | 46        | 41             | YES         | 3        | 1          | LOW        | a. Re-check each source code  
b. Check all cost information content from all campus departments                |
| 17 | Pembukaan RIASEC                  | 56        | 56             | NO          | 1        | 2          | LOW        | a. Make some server improvements                                                 |
| 18 | Detail Konten Komunitas           | 58        | 55             | YES         | 3        | 2          | MEDIUM     | a. Re-check each source code                                                    |
| 19 | Alive youtube                     | 110       | 95             | YES         | 4        | 2          | HIGH       | a. Re-check each source code                                                    |
| 20 | List Tes Activity.set dialog kategori | 30    | 29             | NO          | 1        | 1          | LOW        | a. Make some server improvements  
b. Check the database                                                              |
| 21 | Detail Diskusi Universitas        | 27        | 27             | YES         | 3        | 1          | MEDIUM     | a. Make server improvements                                                     |
| 22 | Send Bird. Get Instance           | 40        | 32             | NO          | 1        | 1          | LOW        | a. Give suggestions (notification) to users to stabilizing the network          |
| 23 | Soal Minat Bakat RIASEC           | 30        | 26             | YES         | 5        | 1          | HIGH       | a. Melakukan cek ulang pada setiap konten soal RIASEC                           |
| 24 | Siswa Komentar                    | 24        | 22             | NO          | 1        | 1          | LOW        | a. Re-check each source code                                                    |
From the results of the discussion, it was found that the Feed section occupied the level of 'High' risk due to a force close and had a very high failure rate of 1181 times but was not a major part of the feature. Study Program Appeal (Banding Program Studi) occupied 'High' level of risk due to force close and had quiet high incidence rate as much as 935 times but was not a major part of the feature. Discussion of the majors test (Tes Penjurusan) had the level of 'High' risk due to the occurrence of a force close gave disadvantages to the users who were reading their test results. The discussion of Tes Pintar had “Low” risk level because there was no force close even though the frequency of events was quite high at 315 times. Pin Point occupied the ‘Low’ risk level because there was no force close and the problem occurred because of a network error that was not the application itself, though the incidence rate reached 245 times. The exercises on Belajar Pintar occupied 'Low' level of risk because there was no force close and not giving any interferences to the user directly even though the occurrence rate was 245 times.
Open Chat was in “Medium” risk level even though there was no force close but this minor failure was quite disturbing the user who wanted to ask while the program was live. University Overview occupied 'Low' risk level because there was no force close and not in the main feature and the occurrence was quite low at 108 times. Undertaking Tes Pintar occupied 'Low' risk level due to no force close in the main part of the features, so it was in “Low” risk level. University Detail Information was in “Low level” because there was no force close and the low occurrence in 84 times. Endless Recycler View Scroll Listener was in “Medium” risk level because of the force close caused by the users scrolling the application too fast but not in the main feature and the occurrence was not that high. Discussion of Interest and Talent (Minat Bakat) occupied the level of 'Low' risk due to non-occurrence force close that was not experienced by the user and the occurrence rate was quite small, 146 times. Minat Bakat/Interest and Talent DISC questions occupied the level of risk 'Very High' due to the occurrence of force close on the main features that made the users unable to use personality test services so it made the main function as a personality test feature errors and really interfere the users. Adapter Work List was in 'Low' risk level because there was no force close that did not interfere the user directly and the occurrence rate was quite low, 123 times. New University was in the risk level 'Moderate because there was no force close but the user started to feel the interference with the error and the frequency of medium failure was 184 times. Department Fee was in 'Low' risk level due to a force close but not in the main feature section and very low occurrence rate of 46 times, and so what happened to other failures in the features section.

After conducting assessment using Excel, it was found the Features Risk Mapping of Aku Pintar application as shown in Figure 2. The risk map was made with a 5x5 matrix, adjusting to the measurement criteria of severity and occurrence. The risk map could be used to determine priorities. This priority was obtained from the results of the impact level or the severity and occurrence level. Divided into 4 risk levels namely 'Very High', 'High', 'Medium', and 'Low'. There was 1 risk with a Very High level of risk. Priority I was number 13. Priority II was number 1 & 2. Priority III is number 3. Priority IV is number 19. Priority V was numbers 7, 15, 11, & 18. Priorities VI were numbers 23 & 31. Priority VII was 28 & 4. Priority VII was numbers 21, 25, 27, 29, 30, 32, 35, 38, 41, 42, 43, 5 & 6. Priority VIII was number 8, 9, 10, 17, 12, 14, 16, 25, 36, 39, & 47. Priorities IX was numbers 20, 22, 24, 33, 34, 37, 40, 44, 45, & 46.

The mitigation plan and the results of brainstorming with experts in the Mobile Developer division of Aku Pintar application could be seen in Table 3 and Table 4. In classifying the level of risk, indirect brainstorming with experts in Mobile Developer division used the Mitigation Interference Report from PT Aku Pintar Indonesia which was the result of brainstorming from the Mobile Developer of Aku Pintar application itself.

![Figure 3. Features Risk Mapping](image-url)
Compilation and determination were carried out and fitted to the objectives of the thesis. Frequency data and Impacted User could be obtained from Google Play Console detection system.

V. CONCLUSION

Through a case study of system errors/bugs in Aku Pintar application, this proved that the proposed methodology shows the ability to assist company management to be able to carry out analysis in a systematic, effective and technical manner. FMEA provides complete documentation of information related to the company to plan and prevent repetitive system errors while improving system performance. FMEA also helps to measure which system errors are the most critical so that it makes it easier to prioritize which system errors should receive greater attention. Mitigation will be more effective if it follows the priorities mentioned in the risk map. In the future, research needs to be done regarding the improvement budget plan so that the funds that come out become more effective.

REFERENCES

[1] W. Rahman and F. Alfaizi, “Mengenal Berbagai Macam Software.” Surya University, Tangerang, 2014.
[2] C. Carlson, Understanding and Applying the Fundamentals of FMEAs. Arizona: ReliaSoft Corporation, 2014.
[3] C. S. Carlson, Effective FMEAs: Achieving Safe, Reliable, and Economical Products and Processes Using Failure Mode and Effects Analysis. Hoboken, N.J.: John Wiley & Sons, 2012.
[4] A. Asllani, A. Lari, and N. Lari, “Strengthening information technology security through the failure modes and effects analysis approach,” Int. J. Qual. Innov., vol. 4, no. 1, Dec. 2018.
[5] A. Corder, Teknik Manajemen Pemeliharaan. Jakarta: Erlangga, 1992.