

IFB398 -
Capstone
Project

20
22

PROJECT REPORT

PHASE 1



PICASSO
TECH

Prepared For :
Alessandro Soro &
Ross Schamburg

Prepared By:
Jessica Quinn
Trisha Dajie
Liam Ferrente
Bella Howard

TABLE OF CONTENTS

1.0	-----	1
1.1	Project Context, Goals & Scope-----	1
1.2	Risk Assessment, Ethics, Mitigation Strategies-----	2
1.2.1	Privacy-----	2
1.2.2	Competitors-----	3
1.2.3	Legalities-----	3
1.2.4	Governance, Feasibility & Ethics-----	3
1.2.5	Risk Assessment-----	4
1.3	Project Requirements-----	5
1.3.1	User Requirement Types-----	5
1.3.1.1	Usability Requirements-----	5
1.3.1.2	User Experience Requirements-----	5
1.3.1.3	User Interface Design Requirements-----	5
1.3.1.4	Functionality of System Features Requirements-----	5
1.3.2	Academic Supervisor Requirements-----	6
1.3.2.1	Educational-based Requirements-----	6
1.3.3	Prioritisation of Requirements-----	6
1.3.3.1	Must Have Requirements-----	6
1.3.3.2	Should/Could Have Requirements-----	7
1.3.3.3	Won't Have Requirements-----	7
1.4	Project Plan & Progress-----	7
1.4.1	Release Plans-----	7
1.4.1.1	Release 1-----	7
1.4.1.2	Release 2-----	8
1.4.1.3	Release 3-----	8
1.4.2	Gantt Chart-----	8
1.4.2.1	Project Progress-----	8
2.0	-----	8
2.1	Architecture-----	8
2.2	Technical Description-----	9
2.2.1	The iPhone-----	9
2.2.2	The Desktop Environment-----	9
2.2.3	Unity-----	9
2.2.4	Key Classes & Methods-----	9
2.3	Functionality-----	9
2.4	Quality & Metrics-----	10
2.4.1	Unit Test-----	10
2.4.2	Acceptance Test-----	10
2.4.3	Code Quality Metrics-----	10
2.4.3.1	Maintainability & Extensibility-----	10
2.4.3.2	Portability-----	10
2.4.3.3	Code Readability & Documentation -----	10
2.4.4	Burndown Charts -----	10
2.4.5	Summary-----	10



TABLE OF CONTENTS

Appendix A - User Stories -----	11
Appendix B - Release Plans-----	13
Appendix C - Gantt Chart-----	16
Appendix D - Risk Assessment-----	17
Appendix E - Risk Matrix-----	19
Appendix F - UML Diagram-----	20
Appendix G - System Architecture-----	20
Appendix H - Terms & Conditions-----	21
Appendix I - Privacy Policy-----	21
Appendix J - Terms & Conditions Checkbox-----	22
Appendix K - Privacy Policy Checkbox-----	22
Appendix L - Home Screen-----	23
Appendix M - Terms & Conditions Config-----	23
Appendix N - PDF Summary-----	24
Appendix O - Burn down Chart as Release Plans-----	26
Appendix P - Burn down Chart as Release Deliverables-----	26
Appendix Q - Unit Testing-----	27
Appendix R - Code Snippet-----	27
Appendix S - Research References-----	27



SECTION 1.0

PROJECT CONTEXT, GOALS, SCOPE & MANAGEMENT



Section 1.1

Project Context, Goals & Scope

For IFB398 – Capstone Project (Phase 1), Picasso Tech sought to complete an academic project for the Queensland University of Technology (QUT) alongside the School of Computer Science supervised by QUT Senior Lecturer within the Faculty of Science, Leonie Simpson. This Capstone Project differs significantly to traditional projects that have been provided to other teams. As our academic supervisor, Leonie provided Picasso Tech with no brief and complete creative freedom to pursue a project that has the overall goal of encapsulating a strong educational undertone with a specific focus on information security. With this freedom, Picasso Tech developed the project idea of an **Application Privacy Analyser** - a desktop application development solution that has been developed specifically for iOS mobile devices. Upon refining the overall goal, the overarching goal of this project is to enhance the educational resources that can be used to assist users in understanding privacy and security across their mobile devices. The aim of this project over both IFB398 and IFB399 – Capstone Project (Phase 2), is to produce a desktop application software that can determine the downloaded applications on an iOS mobile device once the device has been plugged into a laptop or computer. Once scanned, it will gather intelligence regarding the information and data that the applications are collecting from the mobile device. To strengthen educational tone, the application should then be able to collate a visually appealing and informative summary in both interface and PDF formatting. This will detail the collected data and suggest resulting recommendations to assist in maintaining and reinforcing the privacy and security of the phone user through personalised security tips and further informational resources to assist in further understanding information security practices – such as confidentiality, integrity, and availability (CIA).

To produce the **Application Privacy Analyser**, Picasso Tech intends to develop the project artefact using Unity Technologies' cross-platform game engine, 'Unity', which primarily supports video game development and simulation applications for computers, consoles, and mobile devices. In theory, the **Application Privacy Analyser** will be an educational tool that exhibits a straight-forward user journey and provides a navigational user experience through an optimised user interface. This interface then allows users to utilise the resources provided to them to enhance their understanding of their mobile device security by scanning their mobile device and consuming and understanding the presented results and recommendations both immediately within the interface, and via a downloadable PDF summary. In terms of functional technical deliverables, the **Application Privacy Analyser** must deliver the ability to read as well as accept all terms and conditions and privacy policy agreements prior to accessing the main functionalities of the application; the ability to gather and collect a mobile device's application contents; the ability to start the mobile device scan; the ability to present security statistics and tips within the desktop application user interface; the ability to be developed and interacted with as a desktop interface; the ability to generate a comprehensive PDF summary of the device scan's results; the ability to analyse data from applications of the IOS mobile device; the ability to view data from the mobile device through visual and filterable charts and graphs; and the ability to filter applications based on data types. In order to achieve these functional technical deliverables, the **Application Privacy Analyser** must be able to gather data from iOS mobile devices as a result of web scraping, and then correctly input this data with the appropriate features presented within the desktop interface, as well as integrate the correct data within the allotted sections in the downloadable PDF summary. Additionally, the user interface needs to exhibit a seamless user journey with use of interactive elements to ensure users have functional access to all desired elements of the Application Privacy Analyser – such as the device summary, application list, and charts and tables, as well as ensure that no interactive elements lead to a dead-end within the application, interrupting the user behaviour flow.

PROJECT CONTEXT, GOALS, SCOPE & MANAGEMENT



Section 1.1 Project Context, Goals & Scope

Throughout Phase 1, Picasso Tech developed extensive user stories – **Appendix A**, and release plans – **Appendix B**, for the duration of IFB398 and IFB399. While Release Plan 1 details user story five (S05) surrounding web scraping, and user story nine (S09) detailing the development of the desktop environment, Picasso Tech has also been working on components from Release 2 that can be collaboratively developed alongside the user stories outlined in Release 1. This includes actioning the user stories that fall under Release 2's 'Terms and Conditions and Privacy Policy' and 'Cyber Security Guidelines'. Picasso Tech actively decided to begin work on the user stories from Release 2 as many elements could be implemented during the development of S09 and alongside S05. The two main user stories depicted in Release 1 are very technical and labour intensive which indicates why Release 1 focuses solely on these deliverables. However, ensuring that we are implementing elements of Release 2 where applicable ensures that, as a team, Picasso Tech is utilising strong agile project management by prioritising accordingly and continuing to progress with the development of the project.



Section 1.2 Risk Assessment, Ethics, Mitigation Strategies

1.2.1 Privacy

Privacy is an instrumental element to the wellbeing and protection of individuals, and is a right that each human is entitled to. The interpretation of privacy is subject to the context in which it is applied to. Roger Clarke (2014) details elements of privacy relevant to privacy of the person, privacy of personal behaviour, privacy of personal communications, privacy of personal experience, and privacy of personal data – of which is contextually relevant for Picasso Tech.

Privacy of personal data encompasses data privacy and information privacy in conjunction with data protection. This privacy subsection claims that an individual's data should not be readily available to others or organisations, and if that personal data is utilised by a third party, the individual must have a degree of control over the data and its use (Clarke, 2014, p. 177). This is relevant to the data stored by applications on a mobile device as upon downloading an application, many applications ask for permission to collect data from varying device elements, such as the camera, voice recording, camera roll, and files. For social platform applications such as Snapchat, Facebook, and Instagram, allowing permissions for these device elements is required to utilise relevant platform features - such as recording videos or posting photos stored in the camera roll. However, applications such as 'iTorch' – a flashlight application downloadable from the App Store, asking for permissions to the device camera, voice recordings, files, and camera roll does not fall into the necessary scope of functionality for the application, and leaves individuals wondering why such a basic app requires these permissions. Allowing access to these elements of the device gives permissions for mobile applications to potentially access both the front and back camera; record the individual and the screen whenever the application is in use or "open"; take pictures and videos without informing the user as the user has already given consent in system permissions; upload images/videos taken immediately to cloud servers and to third parties; run real-time biometric analysis on the user and store the data (Gibbons, 2018, para. 17). Picasso Tech's **Application Privacy Analyser** assists in mitigating this issue and is being developed to support in identifying which applications are using what information to assist users in becoming aware of what data they are providing to which applications and making the decision as to whether certain applications should be using certain data types.





Section 1.2

Risk Assessment, Ethics, Mitigation Strategies

1.2.2 Competitors

Upon analysing the current market, there are no applications available that offer the exact services as Picasso Tech. Albeit, there are applications that offer varying other elements relative to the information security domain. While these applications are competitors, there is evidence to suggest that these applications can offer great value to a user when used in conjunction with Picasso Tech's **Application Privacy Analyser**. Two notable products include Ostorlab – a commercial application and service that offers an extensive penetration analysis of a client application before or while the application is on the market. Ostorlab analyses the application to find any vulnerabilities or threats within a client's application, and assists in mitigating these issues before the application is sent to market, or updates to an application that is already on the market (Ostorlab, 2022). Additionally, Lumen Privacy Monitor is an academic initiative application made for Android that analyses mobile traffic and assists users in identifying privacy leaks stemming from applications downloaded on a user's device. Lumen Privacy Monitor provides detailed reports on your downloaded applications that have been part of a data leak, identifies traffic patterns and details the private data collected by applications and online services on your device, and provides more extensive information about how each application on your device works and what it connects to (Haystack, 2017).

1.2.3 Legalities

When dealing with sensitive topics such as privacy and the data collection, it is crucial that Picasso Tech is aligned with the challenging legalities surrounding penetrating iOS devices and the collection of data that is presented within the **Application Privacy Analyser**. Picasso Tech acknowledges that there is a fine line separating the legalities surrounding the data collection from mobile devices, particularly with Apple iOS.

However, the Application Privacy Analyser grabs data that has been aligned to the mobile user - not data that is stored by individual applications across the device. The information grabbed includes the system permissions that the user has allowed within the factory 'Settings' application on Apple devices. With this in mind, the Application Privacy Analyser scrapes the iOS device for base layer information, specifically the data types that have been enabled within the system permissions for applications across the device to access. The legalities surrounding use of the Application Privacy Analyser are outlined in the Terms and Conditions and Privacy Policy presented to users upon opening the application. By agreeing to these terms and policy, users allow Picasso Tech to scrape their mobile device for the absolute required information and nothing else, as well as assures users that any collected data will be immediately disposed of upon termination of the session. Additionally, Picasso Tech has considered all elements of the Australian information security standards including - AS/NZS 27005:2012 Information Security Risk Management, AS/NZS 27001:2015 Information Security Management Systems, and AS/NZS 27002:2015 Code of Practice for Information Security Management upon the development, distribution, and use of the **Application Privacy Analyser**.

1.2.4 Governance, Feasibility, and Ethics

Picasso Tech has ensured the implementation of governance in accordance with ISO/IEC 38500 International Standard for Corporate Governance of IT (IT Governance) throughout the entirety of IFB398 and intends to continue to apply for the duration of IFB399 for the Application Privacy Analyser. To ensure governance throughout the project, Picasso Tech acts as the project board to ensure the efficient and effective agile management style of the project, as well as ensuring equal accountability and ownership across the project and the decision making and rights of all members of the project board. By implementing this form of governance, Picasso Tech can work with and provide QUT and Leonie Simpson with project assurance across both internal and external views.



Section 1.2

Risk Assessment, Ethics, Mitigation Strategies

Given Picasso Tech has undertaken an academic project, upon the development of the project idea, the feasibility of the project was a highly analysed criterion. Upon deciding on the **Application Privacy Analyser**, Picasso Tech concluded that the application would provide great value and be greatly beneficial to users in terms of enhancing educational resources and raising awareness as to the types of data that is being collected in the background of user mobile devices by varying applications. Additionally, all elements required to effectively develop this project are feasible. The feasibility of this project has been accounted for in **Appendix C** which outlines the management plan through a Gantt Chart. In developing this, Picasso Tech accounts for the event where the scope of the project may change in accordance to any permission or access restraints, and technical and scheduling restraints in terms of managing the collection of data which has been accounted for task duration times and the project scope. This will be further discussed in depth in **Section 1.2.5**.

It is imperative to ensure that the research conducted as a result IFB398 and IFB399 adheres to ethical standards to avoid any ethical implications throughout any testing or development phases - specifically when research involves inputs from human participants. The scope of development for the **Application Privacy Analyser** involves utilising usability tests on external users. In doing so, Picasso Tech acknowledges and vows to adhere by the universal research ethics principles including; voluntary participation - ensuring all participants are willingly participating; no harm comes to participants; privacy – ensuring the protection of identity for participants through either confidentiality or anonymity; informed consent – participants have a full understanding on all known risks involved and researchers avoid deception and concealment.

The purpose of this is to ensure that participants are aware of their rights when participating in research, as well as ensuring the protection of participants, the honesty, trust, and integrity of the results gathered, and the avoidance of plagiarism and the fabrication of data. For Picasso Tech, ensuring that ethical research principles are followed in IFB399 is imperative as the scope of the project anticipates that prospective research participants are anticipated to utilise their personal IOS mobile devices in order complete usability tests as a result of the final prototype testing.

1.2.5 Risk Assessment

Appendix D presents an extensive and in-depth analysis of 40 relevant risks that have been identified in correlation to Picasso Tech's Application Privacy Analyser. This risk assessment details the varying risk scenarios that are associated with this project artefact for Picasso Tech, QUT as a client, and future potential users as individuals that would be affected through the use of this project artefact. This risk assessment details the identification of the type, the type of risk, the likelihood, impact, consequences and mitigation strategies for each associated risk in depth and considers the possible ethical implications that arise from recruitment research participants. By implementing a risk assessment, Picasso Tech can gather a stronger understanding regarding the overall feasibility of the project, as well as have confidence in knowing that there are methods of mitigation for varying scenarios that may cause issues along the project timeline.

It is imperative that a risk assessment is conducted when conducting any type of project within the industry. This risk assessment consists of five types of risk categories including technology; people; organisational; requirement; and estimation risk. **Appendix E** details the risk estimation tables, where each has been qualitatively measured following the key words 'rare', 'unlikely', 'possible', 'likely', and 'almost certain' for the likelihood of a risk occurring, and 'insignificant', 'minor', 'moderate', 'major', and 'catastrophic' for the impact that the risk would have if it were to occur. Furthermore, this risk assessment was conducted following the input and guidance of the Australian information security standards as discussed in **Section 1.2.3**.



PICASSO
TECH



PROJECT CONTEXT, GOALS, SCOPE & MANAGEMENT



Section 1.3 Project Requirements

Requirements elicitation has been conducted for this project. All user stories are outlined in **Appendix A**. The project's requirements have been developed through the investigation of key solution criteria, system features, and functionalities that are needed to create the desktop software application. Thorough project research as well as analysis of strategic objectives have greatly assisted in the accumulation of solution, transition, and technical-based requirements.

1.3.1 User Requirement Types

Referring to **Appendix A**, the first set of requirements explore the usability of the platform, user experience components, user interface factors, and functionality of the system's features. These requirements have been documented from the users perspective.

1.3.1.1 Usability Requirements

In terms of the user stories that are formed for the usability requirements of the platform, majority of them are configured to deliver ease of learning aspects. These aspects are evident through the adoption of clear messages and alerts that display user friendly directions. This enables users to navigate easily through the application. User story eight (**S08**) regarding the status indicator for the device detection functionality and user story fourteen (**S14**) regarding the error message for system complications, both provide sufficient information to the user about the status of the application's current processes. This is significant to implement as users can be informed about the developments that have been made with the detection of their device and the issues that have occurred. This insight is critical to present within the application as it reduces user confusion and by providing an update or instruction message, allows them to understand what action to perform next, therefore, assisting with the user behaviour flow.



1.3.1.2 User Experience Requirements

There are also a multitude of user stories that address the various user experience components that aim to improve the effectiveness and efficiency of operations throughout the system.

For example, user story three (**S03**) outlines the layout of the device's applications to be displayed in a list view. Presenting the applications in this format can improve the readability of content as well as enhance efficiency through the simple interface design that allows users to easily browse through information.

1.3.1.3 User Interface Design Requirements

In terms of the aesthetics of the application, some user stories have been developed to address the various user interface design requirements. An example of this can be seen in user story twelve (**S12**) which explores the display of user's data usage results in a chart format. The implementation of presenting data in this format would be more aesthetically pleasing compared to a bullet point list of key findings. It is critical to create an intuitive and eye-catching application to build as well as maintain user interaction and engagement levels. The user interface design factors are planned to be exhibited through the display of user data within the application and throughout the PDF summary document.

1.3.1.4 Functionality of System Features Requirements

The final set of user stories required for the user role surround the functionality of the system's features. The functionality of the desktop application's features is highly valuable to emphasise as it can improve the system's performance through the implementation of helpful tools. For example, user story four (**S04**) allows the user to filter and sort the mobile device's application list to their desired data type preference such as 'most data usage' or 'most recent'. This functionality gives the user a choice and preference which can ultimately improve their experience when using the desktop application. Integrating these types of functionality tools and features can create a significant impact in terms of ease of use aspects.



PROJECT CONTEXT, GOALS, SCOPE & MANAGEMENT



Section 1.3 Project Requirements

1.3.2 Academic Supervisor Requirements

The second set of requirements have been recorded from the perspective of the project's Academic Supervisor, Leonie Simpson. Leonie's fundamental requirements surrounds the integration of an additional component that promotes cyber security best practices. This essential stakeholder requirement enabled the project's scope and purpose to transform. After multiple meetings and discussions with Leonie regarding the end goal for the project, the direction of the desktop application's initial capabilities and focus had been modified. The system is now expected to not only gather and analyse mobile application data, but it is also now projected to be built as an educational learning tool. The concept of presenting techniques and strategies for improving security measures within the application, delivers significant value as well as insight for users. Leonie believes this additional component would be highly beneficial for the team to develop and deliver as a considerable feature of the application. This educational-based section would also extend the user behaviour flow within the application. Users can learn about the security of their device which is the main purpose of the system before continuing to educate themselves on the most effective information security practices. The fundamental goal of these requirements would be to improve users overall understanding of key security components, independent of their level of experience or knowledge in the area. Additionally, it would enable them to integrate and adopt their learnings to other devices in the future.

1.3.2.1 Educational-based Requirements

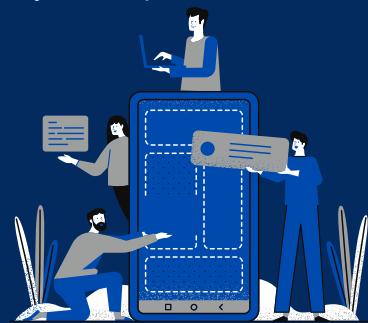
Various educational-based requirements have been configured for the project's Academic Supervisor. These requirements are based on the desktop application's ability to provide a sufficient set of terms and conditions, privacy policy, and cyber security principles. Examples of these can be seen through user story sixteen (**S16**) regarding the application's security measure guidelines and user story seventeen (**S17**) regarding the inclusion of educational information. The development team is required to conduct thorough research from a reliable range of sources to fulfill these requirements.

This would provide credibility to the information and strategies that are produced within the PDF summary report. These user stories create and emphasise the educational learning experience that Leonie desired for the project to include.

1.3.3 Prioritisation of Requirements

1.3.3.1 Must Have Requirements

There has been a strategic prioritisation of user stories designed to effectively address the project's key deliverables and goals. The MoSCoW method has been utilised to assign and prioritise user stories. Picasso Tech has heavily prioritised two user stories which are expected to be commenced at the very beginning of the desktop application development. User story five (**S05**) and user story nine (**S09**) have an estimated forty-eight story points in total and are the only requirements for the first release. Picasso Tech have allocated and classified these requirements as 'Must Haves' as they share the most technically complex set of processes and provide the main functionality of the system. User story five is based on the critical data collection and web scraping procedures that are needed to upload the mobile device's application contents to the **Application Privacy Analyser**. User story nine explores the application's ability to detect and identify a mobile device once connected. Taking into account that these two requirements are high level with multiple technical complexities involved is the reasoning behind them being the only requirements in the first release. This provides sufficient time for the build of these critical functionalities to commence at the beginning of the semester. Additional time can be allotted for them if further developments need to be made or if there is an unexpected delay. To ensure these requirements are delivered on time, project reporting and monitoring will be conducted to determine whether risk treatment plans need to be utilised and if the project scope needs to be modified.





Section 1.3 Project Requirements Continued

1.3.3.2 Should/Could Have Requirements

Picasso Tech chose and assigned the 'Should Have' and 'Could Have' requirements after the 'Must Have' requirements were determined. These are requirements that can potentially be implemented within the desktop application to add more value or features to enhance user experience components. For example, user story fifteen (**S15**) regarding the scanning progress bar, is a feature that could be added to enhance the user's experience as it indicates the status of their mobile device scan which improves the users understanding of the application's processes. The development team has allocated user story fourteen (**S14**) as a 'Should Have' requirement as there are a few technical complexities involved with building the error message functionality for a specific system issue. However, this should be integrated within the application as it is essential to inform the user about the operations involved with their device's content especially when an error occurs.

1.3.2.3 Won't Have Requirements

The 'Won't Have' requirements were allocated by the development team after deliberation of the feature's effectiveness within the application was determined. Picasso Tech has assigned user story nineteen (**S19**) as a 'Won't Have'. User story nineteen has an estimated thirty-two story points and is based on the Man-in-the-middle attack investigation. This investigation would enable the development team to have further insight into whether mobile device applications are collecting more information than stated. Due to the high number of estimated story points allocated for the investigation, other requirements involving the main build of the system were prioritised.



Section 1.4 Project Plan and Progress

1.4.1 Release Plans

The release plans for the *Application Privacy Analyser* can be seen in **Appendix B**. There are 3 releases in total with one hundred and eleven story points combined for the project. Picasso Tech has strategically set up and designed the releases to ensure there is sufficient amount of development time allocated at the beginning of the project. This has been organised in this manner to ensure there is enough time to manage any delays or technical malfunctions that could potentially occur during the development of the application's functionalities. It is intended that the project timeline and scope would be re-adjusted to mitigate the risks involved and to ensure all deliverables can be met by the end of the project. The project's start date is June 13th with the end date being October 14th. Picasso Tech has four members contributing to the project's development with an allocation of two and a half working days per week. The build in particular has an estimated five weeks which deduces that the aim for each release should be fifty story points maximum. Five weeks has been used as the estimated development time as the team has considered the two weeks after the end of Release 3 for application refinement or to resolve any unexpected errors.

1.4.1.1 Release 1

Release 1 features the two main user stories and requirements that contribute to the main build of the desktop application. User story five (**S05**) and nine (**S09**) have a total of forty-eight story points. Release 1 has a start date of Monday 13th June and Friday 22nd July is the delivery date. As mentioned in **subsection 1.3.3.1**, these two 'Must Have' requirements are the most technically complex and significant components of the project. **S05** regarding the uploading of the mobile device's contents to the desktop application, requires Picasso Tech's development team to build various functionalities that can track and collect data usage results of a mobile device. **S09** regarding the detection of a mobile device's connection within the desktop application is another technically advanced concept to develop and integrate. Therefore, due to the complexities involved, these two user stories have been heavily prioritised in the release plan compared to other user story types.



PROJECT CONTEXT, GOALS, SCOPE & MANAGEMENT



Section 1.4 Project Plan and Progress

1.4.1.2 Release 2

Release 2 has the most user story requirements out of all the releases. This release focuses on extending the additional capabilities and functionalities of the desktop application. The overarching goal for this release is based on generating results from the connected device's data, as well as establishing information security policies for the application. Release 2 has a start date of Monday July 25th and delivery date of Monday August 29th. This release consists of eight 'Must Have' requirements and one 'Should Have'. There are three sets of highly critical features within this release. The first set explores the requirements that contribute to the creation of the terms and conditions as well as privacy policy for the application. The second feature is based on the generation of results from the mobile device. This includes presenting the data within the desktop application environment and the PDF summary report. The last set highlights the requirements that contribute to ensuring the application has an educational tone and can be used as an information security learning tool.

1.4.1.3 Release 3

Release 3 involves the implementation of additional application features and functionalities to improve the user's overall experience. Release 3 requirements surround usability and interface design-related aspects. This release has three 'Should Have' requirements and five 'Could Have' requirements with a total of twenty estimated story points. Release 3 has a start date of Tuesday August 30th and delivery date of Friday 7th October. Through the implementation of the additional features, users will be able to easily navigate throughout the application platform, are able to be notified with in-app updates and presented with various extra data statistics.



 PICASSO
TECH

1.4.2 Gantt Chart

A Gantt chart has been created to organise and schedule key project deliverables and milestones. This is critical to develop and follow early within the project to ensure all deliverables are accounted for and have adequate time allocated. The Gantt chart also enables Picasso Tech to understand the requirements that have prerequisites which is important to consider when following the order of task events.

1.4.2.1 Project Progress

The Gantt chart which can be seen in **Appendix C** starts from Monday 13th June and ends Friday 7th October. The first release of the project commences in semester 1 with the development team planning to work on the technical components of the build during the holiday period between IFB298 and IFB399.

By referring to **Appendix C**, the collection of Google request application identifications, Apple requests for privacy, the conversion of data processes, and the desktop environment creation are the first set of tasks that begins in phase 1.

Significant progress has been made in phase 1 regarding the development of the two main 'Must Have' user stories, S05 and S09. This progress is evident through the wireframes, mockups, code quality tests, acceptance criteria tests, and some prototypes of the Graphical User Interface (GUI) that has minor functionalities developed.

SECTION 2.0

Section 2.1 Architecture

SOFTWARE
PROJECT

As seen in **Appendix G**, the application receives data from the iPhone, and exchanges the information to and from RAM memory throughout the running of the program. The application also exchanges information to and from the web server as part of a web scraping exercise. At the conclusion of the programme, the user has the option to download the encrypted PDF summary document, and if they decide to do so, the downloaded PDF document will be stored in the PC's 'Downloads' folder. Once the programme is terminated, all information stored in RAM memory will be erased and hence unretrievable. Thus, ensuring the security of the user's personal information by removing any unencrypted, stored data.



SOFTWARE PROJECT

Section 2.2

Technical Description

Accomplishing the goals of this project will require a variety of technical components working in tandem. The proposed software application will be developed for a **desktop environment** using the game engine **Unity**, for users with **iPhones**.

2.2.1 The iPhone

Apple requires all developers on the App Store to report the privacy practices and types of data their apps may handle. As a result, we can obtain accurate information on the types of data that apps on Apple devices could be collecting. App developers for other platforms – such as Android devices, with different marketplaces – such as the Galaxy Store and Google Play, are not required to provide such information. Consequently, it is completely possible for an app on a non-Apple device to handle different, and unknown, amounts of data, compared to the same app on an Apple device. Thus, the privacy analysis our software aims to provide, can only be accurate for Apple devices. Considering this, and the fact that the Apple iPhone had an Australian market share of over 55% in 2021 (Granwal, 2022), the iPhone was selected as the target device for our application.

2.2.2 The Desktop Environment

An application developed for the desktop environment, as opposed to an iOS app, will have access to greater functionality and is not subject to Apple's strict App Store guidelines. Specifically, obtaining the list of installed applications on an iPhone, by an iPhone app, is disallowed by Apple (Apple Developer Documentation, 2022).

We can circumvent this restriction by developing our software for the desktop environment and scanning the contents of an unlocked iPhone connected via cable. The variety of iTunes clones available (Agarwal, 2022) indicate that it is possible to obtain a list of installed applications on an iPhone, as these applications can display, backup, and restore entire contents of unlocked iPhones. Additionally, the desktop environment allows us to develop the required technical components: Web Scraping and Encrypted PDF Generation.

2.2.3 Unity

Although Unity is primarily used for game development, its cross-platform utility and existing proficiency within the software development team, make it a favourable software development environment. Furthermore, Unity uses the programming language C#, which all software developers for this project have experience using. As a result, Unity will provide us an environment to rapidly prototype ideas, user interfaces, and functionality. Lastly, its cross-platform compatibility allows us to simultaneously build our software application for Windows, Mac, and Linux.

2.2.4 Key Classes & Methods

At this point in the development of the application, the prototype consists of purely the User Interface, as the key classes are yet to be implemented. Throughout the following releases, Picasso Tech expects to develop a program with classes and methods as described in **Appendix F**. All classes are to be static, and the main functionality will occur from within the ClientApp Class. This is where the code for the user interface will be placed and all function calls to other classes. As seen in **Appendix F**, ClientApp will hold a number of variables to temporarily store user data and flags that mark the progress of the user in the application (such as whether their phone has been connected, they have selected a button etc).

ClientApp also stores information for the PDF and summary in the application. The DeviceManager class is responsible for all functionality to do with the iPhone and its data collection. The WebScraper class will retrieve all information about the apps from the Apple Store web page. Once the 'Download PDF' button has been selected from within the application, the PDFButton object from ClientApp will call the GeneratePDF method from the PDFCreator class. This class is responsible for the generation of the PDF document and its password.



SOFTWARE PROJECT

Section 2.3

Functionality

Picasso Tech has made significant progress in managing the development of their prototypes, having developed an interactive prototype utilising their interface wireframes through Marvel App, and working on developing a partially functioning and yet-to-be populated prototype on Unity.

As discussed in **Section 1.4.1**, Release Plan 1 – scheduled to be released on July 22nd, 2022, focuses primarily on the two largest components of this project, **S05** - which focuses on researching and developing the correct method of data scraping on iOS mobile devices, and **S09** – which focuses on the development of the desktop environment interface visually. Given **S09** depicts the visual components of the desktop interface and not populating it, Picasso Tech have made a start on incorporating visual and interactive base components from Release 2 – scheduled to be released on August 29th, 2022. This includes user story one (**S01**) – presenting the user with the Terms and Conditions, user story two (**S02**) – presenting the user with the Privacy Policy, user story twenty (**S20**) – having the user action the Terms and Conditions and Privacy Policy, and **S17** – ensuring an educational tone across the project artefact.

Upon opening the Unity prototype, the user will be presented with a pop-up window with the Terms and Conditions in one tab – **S01** as can be seen in **Appendix H**, and the Privacy Policy in another - **S02** as can be seen in **Appendix I**, and checkboxes at the bottom right of each tab. In order to proceed to use the **Application Privacy Analyser**, the user must select the checkboxes in both tabs – as can be seen in **Appendix J** and **Appendix K**. Upon checking both boxes, the user will automatically be taken to the home screen of the interface which encapsulates **S09** – as can be seen in **Appendix L**. This first functioning prototype will allow the user to click through each button on the home screen, however the content is currently unpopulated. If the user wants to view the Terms and Conditions or the Privacy Policy again, they can click the 'Config' button in the top right-hand corner which will currently present them with the same double tabbed window – as can be seen in **Appendix M**. To exit the application, the user can select 'Quit' in the top right-hand corner next to the 'Config' button. **Appendix N** exhibits the development of the PDF summary that will be customised and downloadable for each user and provides an example of the educational tone that the overall **Application Privacy Analyser** will exhibit throughout the user's experience.

The 'Demo' folder in the directory contains a link to the initial interactive wireframe prototype – 'WireframePrototype.url'. This prototype demonstrates the initial anticipated user experience and user journey of the **Application Privacy Analyser**. This directory also includes a zip file containing the current state of the functioning prototype developed on unity – 'UnityPrototype.zip'. The directory also contains a demonstration video of both the wireframe and Unity prototype in action – 'PrototypeDemoVideo_WireframeAndUnity.mp4'.



2.4.1 Unit Test

Unit testing ensures that all individual parts of a program are working as intended. This aids in the development of new, or modified features as developers can run these tests to verify their changes are working correctly and have not caused issues in other parts of the system.

The development team has implemented the Unity Test Framework within the Unity project. This enables Picasso Tech to create automated unit tests for the used code. The main functionality that exists in the prototype, is the requirement for users to accept the Terms and Conditions and Privacy Policy (the contracts) before they have access to the main application. As such, two unit tests for this process was created. The first ensures that when a user has accepted both contracts, the contracts menu disappears. The second ensures that when a user opens the contracts menu via the config button, that both contracts are unaccepted, and the menu is reopened. Although these are two relatively simple tests for the prototype, it lays the foundations for more, and increasingly complex unit tests for the final artefact.

Appendix Q presents the passing results of the two unit tests via Unity's Test Runner. A code snippet for the unit test is also provided which verifies the intended functionality for when a user has accepted both contracts.

2.4.2 Acceptance Test

To ensure the highest quality design for the interface, Picasso Tech conducted internal acceptance tests with their team members as well as Leonie and her team utilising the wireframe Marvel App prototype. These acceptance tests were conducted utilising a questionnaire and recording participant responses and application navigation observations. The document containing the questionnaire and responses can be found in the '**Data**' folder. During these internal acceptance tests, Picasso Tech participants also received input from voluntary external sources via observation who were not directly recruited to take on acceptance tests. These observations and feedback, however, were also taken into consideration when putting together the test results and considering next steps forward with regarding user interface improvements. Upon presenting this prototype to the Leonie, feedback was provided as a whole across the entire interface design. When presented to internal team members, feedback was provided across the whole interface, however, each member focused their feedback on areas that they were not directly involved with developing.

The general consensus from the acceptance test deduces that there were similar ideas surrounding the quality of the design and suggestions for improvements. The overall comments tell us that added colour to the user interface would be beneficial in highlighting the significant widgets like the scan and download PDF buttons as well as adding an aesthetic to the design. There are a few minor adjustments to be made such as the placement of tab exit buttons and size of font for instructions.

These changes will be made in the next iteration and hence will be seen in the final product. During IFB399, Picasso Tech intends to conduct external acceptance tests in order to gain a wide range of feedback on varying **Application Privacy Analyser** prototypes in order to develop the final result.

2.4.3 Code Quality Metrics

High-quality code increases software longevity, lowers maintenance costs, decreases the chances of creating bugs, and often leads to a favourable user experience (Codegrip, 2020). There are several key metrics that can be explored to evaluate the quality of code, these are: **Maintainability**, **Extensibility**, **Portability**, **Code Readability**, **Documentation**, and **Unit Testing** (Bellairs, 2019; Parasoft, 2022).

2.4.3.1 Maintainability and Extensibility

Maintainability is a measure of how easy and quickly the application can be adapted to required changes. Extensibility refers to the ease in which new features can be added, or existing functionality modified, without impacting the entire product. These factors are assisted by the combination of code readability, documentation, unit testing, and code designed with the principles of good object-oriented programming (OOP) in mind. OOP allows for specific features of software to be isolated, reused, built upon, and hides unnecessary detail.

Although only a small software prototype has been developed so far, the principles of object-oriented programming were employed.

2.4.3.2 Portability

Portability is a measure of platform independency and how usable the same software is in different environments. As discussed, our choice of Unity as our development environment allows us to build our application for the Windows, Mac, and Linux operating systems simultaneously.

2.4.3.3 Code Readability and Documentation

Readable and documented code allows developers to:

- Focus on the content, not the layout of the code
- Understand the overall purpose of sections of code
- Understand the fundamental logic of specific sections of code
- Facilitate copying, changing, and maintaining the code

During the development of our prototype, we followed the coding conventions for C# as outlined by Microsoft. Regarding naming conventions, we used Pascal case for our class names and methods, and we used Camel case for fields. Comments were also used regularly to describe the purposes of code and to document classes and methods. Although we have not created separate documentation outside of the codebase, it will be a straightforward task based on the comments we've left so far, and we plan on providing this with the final artefact.

The code snippet provided in **Appendix R** is from a class called UIManager and is an example of our use of **naming conventions**, **code commenting**, and **method documenting**.

2.4.4 Burndown Charts

Burndown charts are indicative of the project plan timetable. **Appendix O** presents a burn down chart detailing the estimated story points per the 3 release plans, whereas **Appendix P** details the estimated story points as per each release deliverable as set out in the Release Plans in **Appendix B**. The project has a total of 111 story points and is expected to be completed by October 7th, 2022.

2.4.5 Summary

In summary, Picasso Tech has already made sufficient progress on various project deliverables in phase 1. The development team aims to utilise and follow the release plans, document key insights as well as weekly progress, and ensure all requirements are met within the **Application Privacy Analyser**.

*References can be found in **Appendix S**

APPENDIX A - USER STORIES

Story ID	As a	I want	So that	Acceptance Criteria	Estimation	Priority
S01	User	to be presented with the terms and conditions	I can ensure I understand all the processes involved within the privacy application	Given I have connected my device and I wish to run the application,	\$1	Must
S02	User	to be presented with the privacy policy		When I read the application's terms and conditions,		
S03	User	to view a list of my devices downloaded apps within the software application		Then I can consent to the terms and conditions before running the application.		
S04	User	to filter the apps based on what data has been shared	I can see what types of data my apps are collecting	Given the privacy policy is readily available,	\$1	Must
S05	User	my device's application data and usage to be loaded onto the privacy application		When I read how this application uses my data,		
S06	User	to click on a button that generates the results		Then I can consent to the privacy policy before running the application.		
S07	User	to click on a button that generates a pdf document	I can view a summary of the data that has been collected in a way that I can export	Given the applications loaded onto the device are compiled into a list,	\$2	Must
S08	User	a status indicator to see whether a device has successfully been detected		When I want to sort the order of applications by type,		
S09	User	to be able to plug my device into my computer		Then I am able view the list in a reordered list based on my selected data type preference.		
S10	User	to see information regarding the implications of data collection	I can make informed choices about the apps I use	Given the privacy application can access my data,	L32	Must
S11	User	to be able to see my suggestions from the analytics report findings		When I press the 'Scan' button,		
S12	User	to be able to view my data usage using charts		Then the privacy application can download my device's application and usage data.		
S13	User	to view the amount of time that I have spent on each application	I am aware of the usage time to data collected ratio.	Given there is a successful connection to a device,	M8	Must
S14	User	a descriptive error message to appear when there is something wrong		When I click on the 'Scan' button,		
S15	User	to see the progress of my device being scanned		Then I am able to trigger the scan on my device.		
S16	Cybersecurity Supervisor (Leonie Simpson)	the application to follow the correct cybersecurity measures and guides	I can ensure the application's processes are aligned with the relevant security standards and principles.	Given the device scan has been completed,	L16	Should
S17	Cybersecurity Supervisor (Leonie Simpson)	the application to be educational (e.g. cyber security principles)		When I press the 'Generate Report' button,		
				Then a PDF will be generated and viewable.		
				Given a device has been successfully connected,	S1	Could
				When I locate the status indicator,		
				Then I can see whether the device connection was successful or not.		
				Given my device has been connected to my computer,	L16	Must
				When I access the application,		
				Then I will be able to use the software application		
				Given the scan has been completed,	S1	Should
				When I view the scan output,		
				Then I will be able to view information regarding the implications of data collected.		
				Given I have various applications on my device,	M4	Could
				I want to ensure that the applications I use do not		
				Then I can make decisions on the applications I		
				Given my device has successfully scanned,	M8	Must
				When the analytics of the application has been compiled		
				Then I will be presented with the information through charts and graphs.		
				Given I can view individual app data,	S2	Could
				When I view an apps time usage,		
				Then I can see the ratio between usage time to amount of data collected.		
				Given the program has been functioning properly,	M4	Should
				When there is an issue within the program		
				Then an error message will be presented to the user.		
				Given my device is being scanned,	S2	Could
				When I can view a progress,		
				Then I know that there has been an issue while analysing my phone.		
				Given the functionality of the application,	M4	Must
				When I check the build and backend system,		
				Then I want to be able to confirm that all processes within the development of the application are setup correctly.		
				Given the applications interprets data,	S1	Must
				When users view the applications results,		
				Then they will be presented with educational information.		



APPENDIX A - USER STORIES

S18	Cybersecurity Supervisor (Leonie Simpson)	the pdf to be encrypted	when a user downloads the document it is secured on their device.	Given a user tries to open the pdf, When they enter the password, Then the pdf will open if the password is correct.	M4	Could
S19	Cybersecurity Supervisor (Leonie Simpson)	the application to perform a Man in the Middle investigation	users can see the accuracy of the data collected.	Given an application is analysed, When a Man in the Middle investigation is conducted, Then users will be able to see whether apps are collecting more information than stated.	L32	Won't
S20	Cybersecurity Supervisor (Leonie Simpson)	Users to complete an action to agree to the Terms and Conditions, and Privacy Policy	I know users have seen the Terms and Conditions and Privacy Policy	Given the Terms and Conditions and Privacy Policy appear when first opening the application, When a user scrolls to the end of the T&Cs and Privacy Policy and accepts, Then they can continue with the application's services.	S2	Must

Story Size Legend	
Small (S)	1 & 2
Medium (M)	4 & 8
Large (L)	16 & 32
Must	
Should	
Could	
Won't	

Release Plan

Release 1: Desktop Application Development

Delivery date: 22/7/22

Total Story Points: 48

The fundamental goal of this release surrounds the main build of the desktop privacy analyser application. These critical features will enable the main functionality of the project to be developed.

Device Application Upload

This feature assists with the privacy application's ability to scan and upload a mobile device's application contents. Processes involving the gathering and collating of application and data usage statistics will be utilised for this area.

Story ID	Story Title	Story Points
S05	Scan Device Application and Usage Data.	32
Story Point Sub-Total:		32

Desktop Environment Creation

This feature enables the application to be accessible and built for a desktop environment. This environment type is critical for the scan to work successfully.

Story ID	Story Title	Story Points
S09	Development of Desktop Environment.	16
Story Point Sub-Total:		16

APPENDIX B - RELEASE PLAN

Release 2: Generating Device Results & IS Policies

Delivery date: 29/08/22

Total Story Points: 43

The overarching goal for this release focuses on generating results from the connected device's data, as well as focusing on information security policies within the application. In doing so, these IS policies ensure that the application adheres to cybersecurity guidelines and measures and enforces user awareness and understanding of the application's terms and conditions and privacy policy.

Terms and Conditions and Privacy Policy

This feature will ensure that users will be presented with the terms and conditions upon first opening the application. In doing so, this feature will require users to scroll through both the Terms and Conditions, and Privacy Policy before proceeding with using the application.

Story ID	Story Title	Story Points
S01	Presenting Terms and Conditions	1
S02	Presenting Privacy Policy	1
S20	Actioning Terms and Conditions and Privacy Policy	2
Story Point Sub-Total:		4

Generating Device Results

Users will be presented with the results generated from their device through varying presentation styles, such as within the application as well as through a downloadable PDF in digestible formats.

Story ID	Story Title	Story Points
S04	Filtering Data	2
S06	Generating Results in Environment	8
S07	Generating Results within PDF	16
S12	Presenting Chart and Table Results	8
	Story Point Sub-Total:	34

Desktop Environment Creation

This feature enables the application to be accessible and built for a desktop environment. This environment type is critical for the scan to work successfully.

Story ID	Story Title	Story Points
S09	Development of Desktop Environment.	16
	Story Point Sub-Total:	
	16	



APPENDIX B - RELEASE PLAN

Release 3: Additional App Features and Functionalities

Delivery date: 7/10/22

Total Story Points: 20

Additional App Features & Functionalities

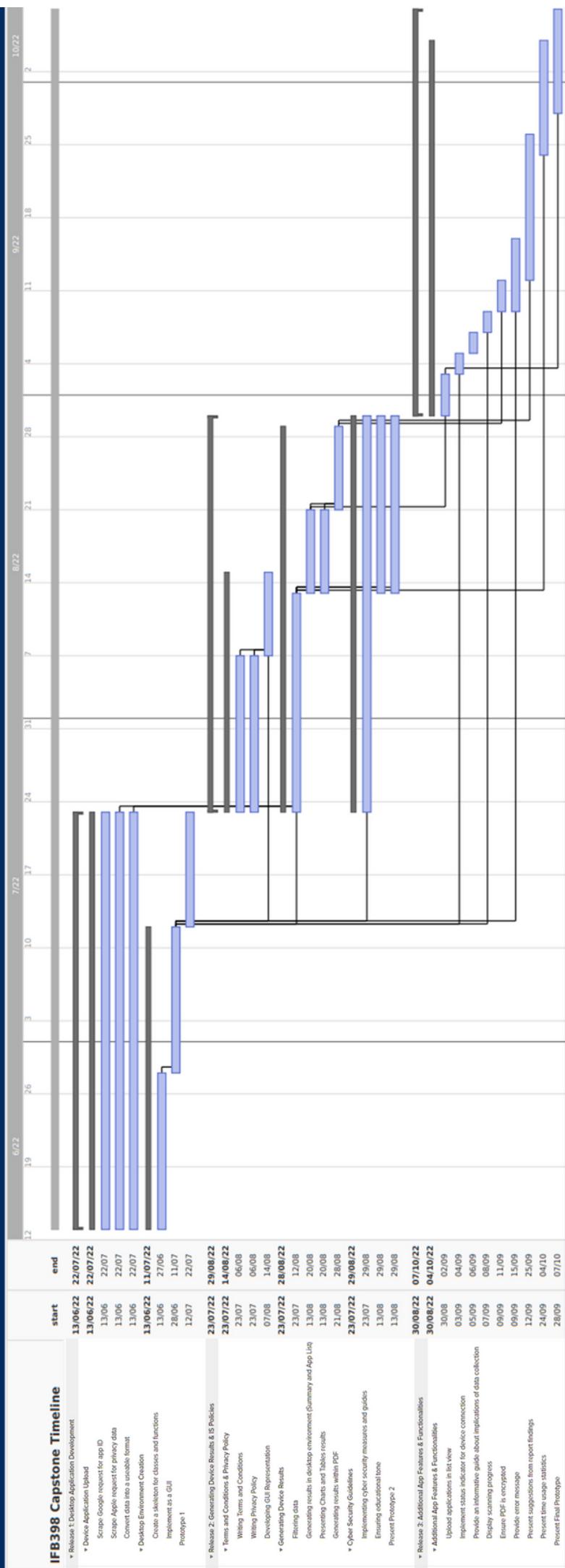
The aim of this release is to provide additional functionalities that improve the user's experience within the application. These set of features surround usability and interface design-related aspects. Through the implementation of these features, users will be able to easily navigate throughout the application platform, are able to be notified with in-app updates, and presented with their device's data statistics as well as informative security practices. Overall, all the features add value towards the application's functionality and capabilities.

Story ID	Story Title	Story Points
S03	Upload Applications in a List View	2
S08	Implement Status Indicator for Device Connection	1
S10	Provide an Informative Guide About Implications of Data Collection	1
S11	Present Suggestions from Report Findings	4
S13	Present Time Usage Statistics	2
S14	Provide Error Message	4
S15	Display Scanning Progress	2
S18	Ensure PDF is Encrypted	4
	Story Point Sub-Total:	20

Release 1		Release 2		Release 3		<ul style="list-style-type: none"> Must Should Could Won't 	
Desktop Application Development		Generating Device Results & IS Policies		Additional App Features & Functionalities			
Story #	Est.	Story #	Est.	Story #	Est.		
S05	32	S01	1	S03	2		
S09	16	S02	1	S08	1		
		S04	2	S10	1		
		S06	8	S11	4		
		S07	16	S13	2		
		S12	8	S14	4		
		S16	4	S15	2		
		S17	1	S18	4		
		S20	2				
SUM = 48		SUM = 43		SUM = 20			
Monday June 13	Friday July 22	Monday July 25	Monday August 29	Tuesday August 30	Friday October 7		



APPENDIX C - GANTT CHART



APPENDIX D - RISK ASSESSMENT

Risk ID	Category	Risk Description	Likelihood	Impact	Consequence	Mitigation Strategy	Owner
R1	Estimation Risk	The scope of the project is larger than anticipated.	Possible	Moderate	Some impactful requirements may have to be removed from the project scope.	Risk Acceptance - Accept the risk, and re-evaluate the scope against the remaining timeline by re-prioritising requirement priorities. Fall Back - Implement back up plan where either a search bar for users to add applications manually to the interface is available or through a ready made list of the most popular apps so that users can tick app options.	Liam Ferrante (Lead Developer) / Jessica Quinn (Internal Project Manager)
R2	Technology Risk	Data scraping does not work for the project.	Possible	Major	Project scope and outcome will not be as extensive as anticipated.		Liam Ferrante (Developer)
R3	Technology Risk	The project scope changes.	Possible	Moderate	Already completed work may now be redundant. More requirements may be added to the project, thus increasing time and capacity pressure.	Risk Acceptance - Accept the risk and update the scope of the project with the new requirements. Re-evaluate requirement prioritisation to cater to updated requirements.	Jessica Quinn (Internal Project Manager)
R4	People Risk	Academic supervisor becomes temporarily unavailable (eg: develops an illness).	Unlikely	Moderate	Replacement supervisor may have conflicting opinions regarding the direction of the project. Our project and its features may deviate from the expectations of the original supervisor.	Fall Back - Academic supervisor has stated they should be able to assign a suitable replacement for the interim.	Bella Howad (Client Lead)
R5	People Risk	A team member may become temporarily unavailable (eg: develops an illness).	Unlikely	Moderate	Project milestones are at risk of not being achieved on time and the project may fall behind.	Reduce Risk - Appoint secondary roles to other team members such that they can resolve any pertaining issues during the interim of unresponsiveness. Additionally, team members should be having regular meetings or regular communication methods to ensure unavailable team member is aware of the continued progress of the project and tasks.	Jessica Quinn (Internal Project Manager)
R6	People Risk	A team member may drop out of IFB398 or stop responding to team messages or stop attending team meetings.	Rare	Major	The project deadlines and goals are at high risk of being missed and the quality of the project features may suffer.	Share Risk - Consult tutor, unit coordinator, and supervisor. Discuss a potential reduction in scope or required features to implement within the project. Work to seek a replacement team member if possible.	Jessica Quinn (Internal Project Manager)
R7	Organisational Risk	Client stops responding to communication by Capstone team.	Unlikely	Major	The project may suffer as a result from delayed feedback or postponed collaborative efforts that are required as part of an assessment piece for the Capstone team.	Avoid Risk - Ensure that the client team is aware of the commitment to regular communications with the Capstone team. Have the client team sign a document adhering to regular virtual/in-person meetings, and ensure follow up emails are sent to the client following each meeting with discussed deadlines.	Bella Howad (Client Lead)
R8	Organisational Risk	Client drops out of IFB398 and IFB399 leaving the Capstone team without a client partner.	Rare	Major	Capstone team does not have a client team to continue the project with. Possible work that has been done for the client may be insignificant. Capstone team grades and project progress may suffer significantly.	Avoid Risk - Ensure that the client team is aware of the commitment that is IFB398 and IFB399. Have the client team sign a document stating that they will participate for the duration of both IFB398 and IFB399.	Bella Howad (Client Lead)
R9	Technology Risk	Platform that the project is being built on experiences a long-term maintenance period.	Rare	Major	Capstone team will be unable to make any progress with the development of the project artefact. The project may suffer missed deadlines for both the client and assessment periods.	Fall Back - Ensure that there is a backup platform where the project and its functionalities can be replicated.	Liam Ferrante (Lead Developer)
R10	Requirements Risk	Miscommunication between client and Capstone team surrounding requirements or feedback to the project artefact.	Possible	Minor	Some of the work that had been completed may have been made redundant or will need to be re-worked to cater to the communicated requirement.	Reduce Risk - Ensure that all requirements are communicated between the client team and the Capstone team through verbal and written communication. Seek approval from client for all work that has been completed before moving onto next milestone task. If the miscommunicated work has already been completed, re-evaluate the requirements of the project together in order to understand what went wrong and navigate the capacity to implement communicated requirement.	Bella Howad (Client Lead) / Trisha Dajie (Report Lead)
R11	People Risk	Participants pull out of completing usability tests.	Possible	Minor	The prototype being tested will have less feedback for improvements.	Avoid Risk - Ensure all research participants are aware of all the requirements of the usability tests and all risks involved before allowing them to begin the usability tests. Have research participants adhere to consent forms before participating, but accept if the participant is adamant about leaving the testing period.	Trisha Dajie (Report Lead)
R12	Estimation Risk	Prototypes receive a significant amount of negative feedback.	Possible	Moderate	The project requirements and project scope may need to be re-evaluated.	Accept Risk - The project requirements and project scope may need to be re-evaluated in conjunction with the feedback received from the usability tests and amended to fit with the received feedback.	Trisha Dajie (Report Lead)
R13	People Risk	The skillset of team members are not enough to complete the project.	Unlikely	Major	The project will not be able to be completed to the standard that had been agreed upon. The scope of the project may have to significantly change and the requirement deliverables may not be feasible.	Avoid Risk - Ensure that the team discusses individual skillsets and passions before embarking on or accepting a project for IFB398 and IFB399. Ensure the project that is accepted or developed is achievable given the responses from the Capstone Team.	Jessica Quinn (Internal Project Manager) / Trisha Dajie (Report Lead)
R14	Technology Risk	Privacy Application Analyser causes technical difficulties/damage to user's device in scanning.	Rare	Catastrophic	This will damage the reputation of the Capstone team as well as QUT. This event will cause physical damage to a user or research participant's personal device and may result in legal action. This is also an ethical issue as the project artefact for user's should bring no harm to users.	Avoid Risk - Ensure that Picasso Tech states that they are not liable for any damages that occur to personal devices and/or artefacts in the Terms and Conditions and Privacy Policy that user's agree to before using the Application Privacy Analyser.	Bella Howard (Client Lead) / Trisha Dajie (Report Lead)
R15	Technology Risk	User's phone scan does not present any results.	Unlikely	Minor	User may not be able to scan their device with the Application Privacy Analyser.	Reduce Risk - See that user's check their system permissions and requirements to ensure that the device 'trusts' the desktop environment that they are plugging their phone into. If that does not work, implement troubleshooting methods. If that does not work, the phone may not be compatible with the Application Privacy Analyser.	Liam Ferrante (Lead Developer)
R16	Technology Risk	Application Privacy Analyser does not dispose of user data after session termination.	Unlikely	Catastrophic	This is a violation of the Terms and Conditions and the Privacy Policy that the user agrees to before using the artefact. Legal action can be taken for violation of the Terms and Conditions on Picasso Tech's behalf.	Avoid Risk - Implement a factory reset of the Application Privacy Analyser each time the session terminates or the program closes. This will ensure that the applications reverts back to a completely 'new' program when opened again.	Liam Ferrante (Lead Developer) / Bella Howard (Client Lead)
R17	Technology Risk	Application Privacy Analyser may not be compatible with some user devices.	Likely	Insignificant	Some users may not be able to scan their devices if they have an older model of iOS mobile devices.	Accept Risk - Develop the artefact to ensure that it works with the most recent and most popular iOS devices that are used today, as the hardware used in older models of phones are different to those used today - some hardware and software will not be updated or compatible with elements utilised within the Application Privacy Analyser.	Liam Ferrante (Lead Developer) / Bella Howard (Client Lead)
R18	Estimation Risk	Capstone team is unable to produce all the 'Must Have' requirements in time for the set deadlines.	Unlikely	Moderate	The non-negotiable components for the project artefact are not delivered on time and the late completion of these elements may have long term impacts on feedback and other deadlines.	Avoid Risk - Ensure that the time allocations to complete each task are correct and realistic.	Trisha Dajie (Report Lead) / Bella Howard (Client Lead)
R19	Estimation Risk	Some 'Must Have' requirements are not delivered as part of any Release Plan.	Unlikely	Major	The non-negotiable components for the project artefact are not delivered - this means that the project will not have all the required functioning deliverables.	Avoid Risk - Ensure that the time allocations to complete each task are correct and realistic.	Trisha Dajie (Report Lead) / Bella Howard (Client Lead)
R20	Estimation Risk	Release Plans are not adhered to.	Unlikely	Major	This results in reputational damage to Qut if the delays are not communicated in an orderly and timely fashion and justified.	Reduce Risk - Ensure that the time estimations for each Release Plan is correct and realistic.	Trisha Dajie (Report Lead) / Bella Howard (Client Lead)
R21	Estimation Risk	Some 'Could Have' / 'Should Have' requirements may not be delivered as part of their allocated Release Plan.	Unlikely	Minor	The project artefact will not be delivered some of its 'desired but not essential' elements on time, and the deliverables will be delayed.	Reduce Risk - Work to avoid this happening by having realistic and correct time estimations.	Trisha Dajie (Report Lead) / Bella Howard (Client Lead)

APPENDIX D - RISK ASSESSMENT

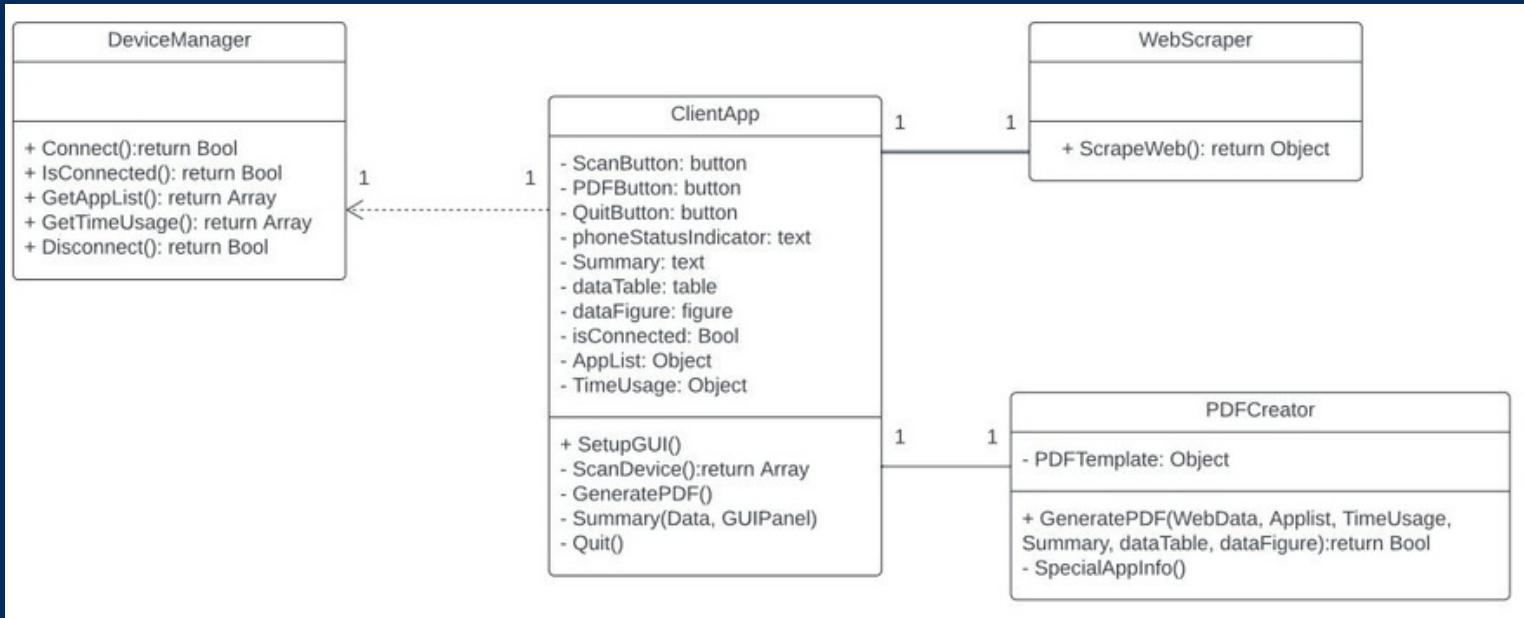
R22	Estimation Risk	Some 'Could Have' / 'Should Have' requirements may not be delivered as part of any Release Plan.	Unlikely	Moderate	The project artefact will not be delivered some of its 'desired but not essential' elements.	Reduce Risk - Work to avoid this happening by having realistic and correct time estimations. Also communicate to the client at the beginning of the project that 'Should Have' and 'Could Have' requirements are the first requirements to be taken out of the project should Picasso Tech face any time constraints or requirement constraints. Avoid Risk - Ensure that there is adequate communication between the client team and the Capstone team. This allows for further understanding regarding what the client team are envisioning and the capacity that the Capstone has to deliver these requirements. Requirements that may be too ambiguous should also be communicated to the client team. Avoid Risk - Ensure that the development roles on the Capstone team are saving each rendition of the project artefact as backup files after each requirement is implemented into the project artefact. Additionally, ensure that are extra backup files stored on either an additional cloud or external hard drive.	Trisha Dajie (Report Lead) /Bella Howard (Client Lead)
R23	Requirements Risk	The requirements provided are too ambiguous, leaving them open to misinterpretation and not meeting the developed requirements.	Possible	Major	Client may have envisioned a different outcome to what the Capstone team produces as part of a requirement deliverable.	Avoid Risk - Ensure that there is adequate communication between the client team and the Capstone team. This allows for further understanding regarding what the client team are envisioning and the capacity that the Capstone has to deliver these requirements. Requirements that may be too ambiguous should also be communicated to the client team. Avoid Risk - Ensure that the development roles on the Capstone team are saving each rendition of the project artefact as backup files after each requirement is implemented into the project artefact. Additionally, ensure that are extra backup files stored on either an additional cloud or external hard drive.	Trisha Dajie (Report Lead) /Bella Howard (Client Lead)
R24	Technology Risk	Project artefact file/s corrupt.	Unlikely	Major	The project artefact progress is lost and the Capstone team will have to restart the artefact development.	Avoid Risk - Make sure that there is a shared cloud drive, such as OneDrive, that the Capstone team can collaboratively store all documents in. This ensures that there is a backup stored on local drives of individual team members, but there is also a backup stored on the cloud so that all team members are able to access the documents.	Liam Ferrante (Lead Developer) / Bella Howard (Client Lead)
R25	Technology / People Risk	Files are stored locally on a team member's drive and the files are deleted.	Possible	Major	The project artefact and Capstone documents are unable to be restored once being permanently deleted from a team member's local drive. This puts the Capstone team back at square one to redo the lost work.	Avoid Risk - Make sure that there is a shared cloud drive, such as OneDrive, that the Capstone team can collaboratively store all documents in. This ensures that there is a backup stored on local drives of individual team members, but there is also a backup stored on the cloud so that all team members are able to access the documents.	Jessica Quinn (Internal Project Manager)
R26	Technology / People Risk	Participants do not have a compatible iOS device in order to complete usability tests.	Possible	Minor	The user will not be able to use the Application Privacy Analyser.	Avoid Risk - older models of iOS mobile devices have older hardware and software that will not be compatible with the updated software and hardware used to develop the Application Privacy Analyser. Reduce Risk - Ensure to have comprehensive and clear discussions with the client when discussing the project requirements to ensure both the client team and the Capstone team have the same vision for the requirements for the project artefact. Be sure to follow up the requirements in written communication after discussion with the client as a record.	Liam Ferrante (Lead Developer)
R27	Requirements Risk	The outcome of the project does not meet the expected requirements.	Unlikely	Major	The client is not pleased with the end result of the requirements implemented in the project artefact.	Accept Risk - Make sure that there is a shared cloud drive, such as OneDrive, that the Capstone team can collaboratively store all documents in. This ensures that there is a backup stored on local drives of individual team members, but there is also a backup stored on the cloud so that all team members are able to access the documents.	Trisha Dajie (Report Lead) /Bella Howard (Client Lead)
R28	Organisational Risk	The client team changes the scope of the project close to the end deliverable deadline.	Possible	Major	Some elements of the project may become redundant with the change in project scope in terms of requirements and deliverables. This will also potentially add a significant increase in time on the project thus making it possible that the project will miss the deadline and fall behind schedule.	Reduce Risk - Ensure to have comprehensive and clear discussions with the client team to discuss any possible changes in scope down the project timeline and see if they can be implemented through regular communication throughout the project duration.	Trisha Dajie (Report Lead) /Bella Howard (Client Lead)
R29	Technology Risk	Users may not have the required platform in order to download and run the project artefact on their own laptops or computers.	Possible	Minor	Users may have to download the platform that the project artefact was built on in order to use the artefact.	Reduce Risk - Find a platform that allows the Capstone team to export the project artefact as a stand-alone element that does not require a background platform to be downloaded in order to use it.	Liam Ferrante (Lead Developer)
R30	Technology Risk	Users may not have a desktop environment to use the project artefact on.	Possible	Minor	This will reduce the prospective users for the Application Privacy Analyser as the project artefact has not been developed for use on mobile devices, and has only been developed for use on desktop environments such as PCs and laptops.	Accept Risk - Make it clear that the Application Privacy Analyser is only desktop and laptop use only for the foreseeable future.	Trisha Dajie (Report Lead)
R31	Estimation Risk	The project violates legal requirements in terms of data scraping and data collection.	Possible	Catastrophic	The project artefact will be utilising techniques that are deemed illegal in some areas of the world and legal in other areas of the world. If the Capstone team are developing the artefact in an area where the methods used to develop this	Avoid Risk - Extensive research is required to ensure that all the procedures - such as data scraping, are being executed in a legal manner prior to beginning the project.	Liam Ferrante (Lead Developer) / Bella Howard (Client Lead)
R32	Estimation Risk	The completed project violates newly implemented privacy / data legal requirements.	Possible	Catastrophic	The Capstone team could face significant legal action if the artefact is being used and the methods used to develop the artefact fall into the category of newly illegal practices.	Avoid Risk - Extensive research is required to ensure that all the procedures - such as data scraping, are being executed in line with the newly implemented requirements.	Liam Ferrante (Lead Developer) / Bella Howard (Client Lead)
R33	People Risk	Users do not agree to the Terms and Conditions or the Privacy Policy upon using the Application Privacy Analyser.	Possible	Insignificant	Users who do not agree to the Terms and Conditions and the Privacy Policy will not be able to use the Application Privacy Analyser.	Accept Risk - It is the user's choice as to whether or not they accept the Terms and Conditions and the Privacy Policy.	Jessica Quinn (Internal Project Manager)
R34	People Risk	Privacy and consent agreement between research participants is broken.	Rare	Catastrophic	Consent agreements are legal documents that have significant consequences if broken resulting in legal action as this can lead to defamation and other legal developments.	Avoid Risk - Ensure to adhere to all storage and security requirements for research recruitment participation.	Jessica Quinn (Internal Project Manager)
R35	Technology Risk	Users may experience errors while using the Application Privacy Analyser.	Unlikely	Moderate	The user may become frustrated when presented with an error message and may want to cease using the Application Privacy Analyser.	Reduce Risk - Write a user guide and a troubleshooting guide to assist users in using the project artefact as well as solving any common errors that may occur when using the project artefact.	Trisha Dajie (Report Lead)
R36	Technology Risk	Application Privacy Analyser does not recognise a device when plugged in.	Possible	Moderate	The user may not be able to utilise the Application Privacy Analyser with their own device. This may be an issue on the project artefact side, or it may be subject to the device that the user is using.	Reduce Risk - write a troubleshooting guide that may assist in fixing the inability to scan a device - such as restarting the project artefact, restarting the desktop environment, and restarting the user device.	Trisha Dajie (Report Lead)
R37	Technology Risk	Application Privacy Analyser may present inaccurate results.	Possible	Major	The Application Privacy Analyser reports incorrect results after scanning a user's device thus presenting the user with the incorrect resulting and presenting them with potentially misleading information that could cause reputational damage.	Avoid Risk - Implement extensive testing with varying devices to ensure that the project artefact exhibits a 100% accuracy rate.	Liam Ferrante (Lead Developer) / Bella Howard (Client Lead)
R38	People Risk	User keeps Application Privacy Analyser open on desktop environment and does not terminate the session upon completion.	Possible	Moderate	Other individuals may use the same desktop environment and may peruse the data that has been left in the project artefact - this is an invasion of privacy and violate confidentiality.	Avoid Risk - Have the project artefact close automatically after 5 minutes of unresponsiveness.	Liam Ferrante (Lead Developer) / Bella Howard (Client Lead)
R39	Technology Risk	The terminate button does not close the Application Privacy Analyser.	Unlikely	Moderate	If the terminate button does not close the application, then other users may be able to peruse the information left in the project artefact.	Avoid Risk - Make the project artefact compatible with the force restart functions - control, alt and delete.	Liam Ferrante (Lead Developer) / Bella Howard (Client Lead)
R40	Estimation Risk	Project artefact is not fully completed by the end deadline of IFB399.	Unlikely	Major	The project is not fully completed by the discussed and approved end date. This will have significant impact on the marks obtained by the Capstone team and the client team will have an incomplete project artefact which goes against the requirements of IFB399.	Avoid Risk - If it is looking likely that the project will not be completed by the project deadline, ensure to have a conversation with the client team to discuss changes to the scope, re-evaluate the priorities of requirements and cater to what can be achieved in for the final deliverable of the project artefact.	Jessica Quinn (Internal Project Manager) / Bella Howard (Client Lead) / Trisha Dajie (Report Lead)

APPENDIX E - RISK MATRIX

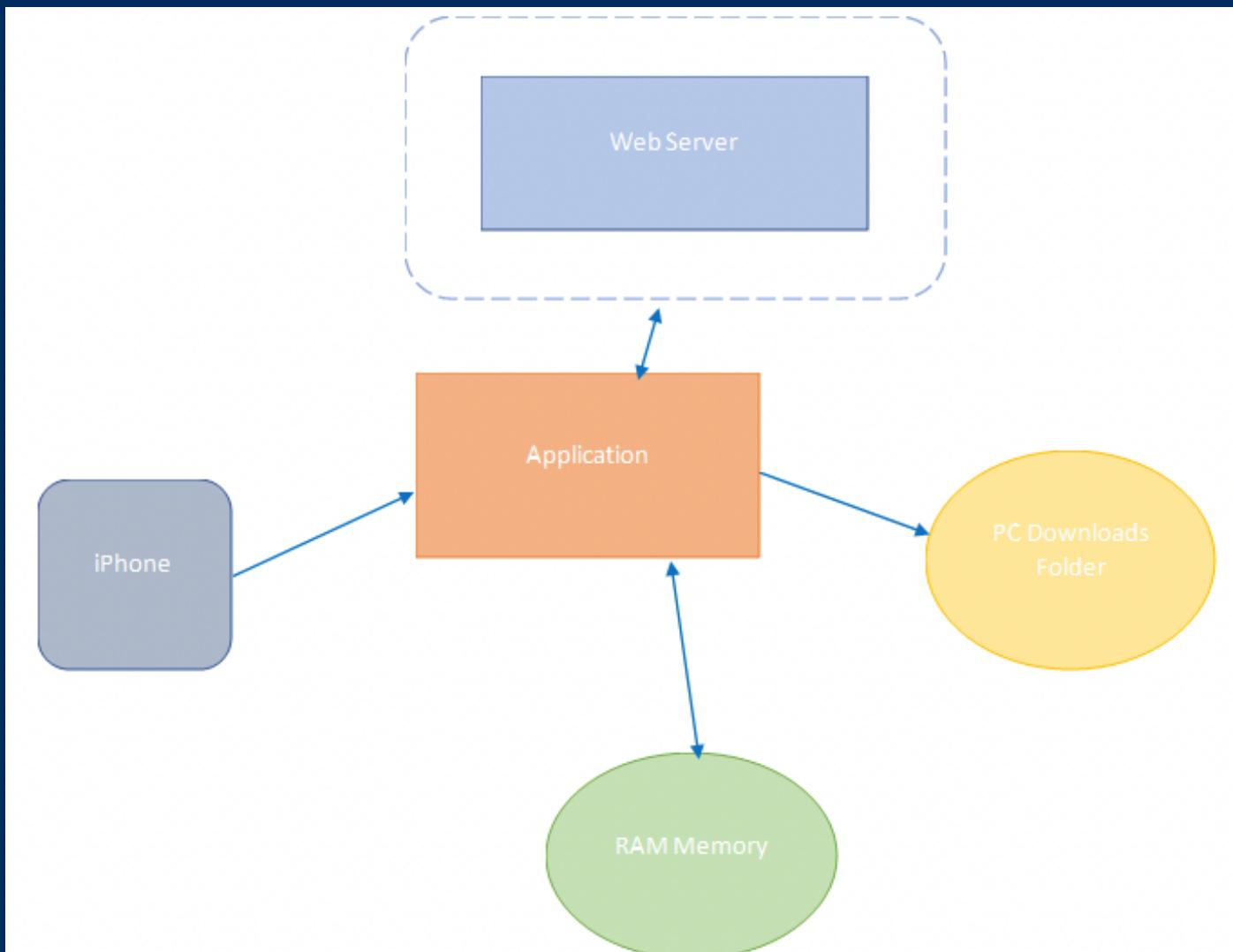
LIKELIHOOD (probability) How likely is the event to occur at some time in the (Linear Scale time specific matrix)	CONSEQUENCES				
	Insignificant	Minor	Moderate	Major	Catastrophic
No Injuries First Aid	Some First Aid required	External Medical	Extensive injuries	Death or Major Injuries	
No Envir Damage << \$1,000 Damage	Low Envir Damage << \$10,000 Damage	Medium Envir Damage <<\$100,000 Damage	High Envir Damage <<\$1,000,000 Damage	Toxic Envir Damage >>\$1,000,000 Damage	
Almost certain - expected in normal circumstances (100%)	MODERATE RISK	HIGH RISK	HIGH RISK	CRITICAL RISK	CRITICAL RISK
Likely - probably occur in most circumstances (10%)	MODERATE RISK	Moderate RISK	HIGH RISK	HIGH RISK	CRITICAL RISK
Possible - might occur at some time. (1%)	LOW RISK	Moderate RISK	HIGH RISK	HIGH RISK	CRITICAL RISK
Unlikely - could occur at some future time (0.1%)	LOW RISK	Moderate RISK	Moderate RISK	HIGH RISK	HIGH RISK
Rare - Only in exceptional circumstances 0.01%)	LOW RISK	LOW RISK	Moderate RISK	Moderate RISK	HIGH RISK



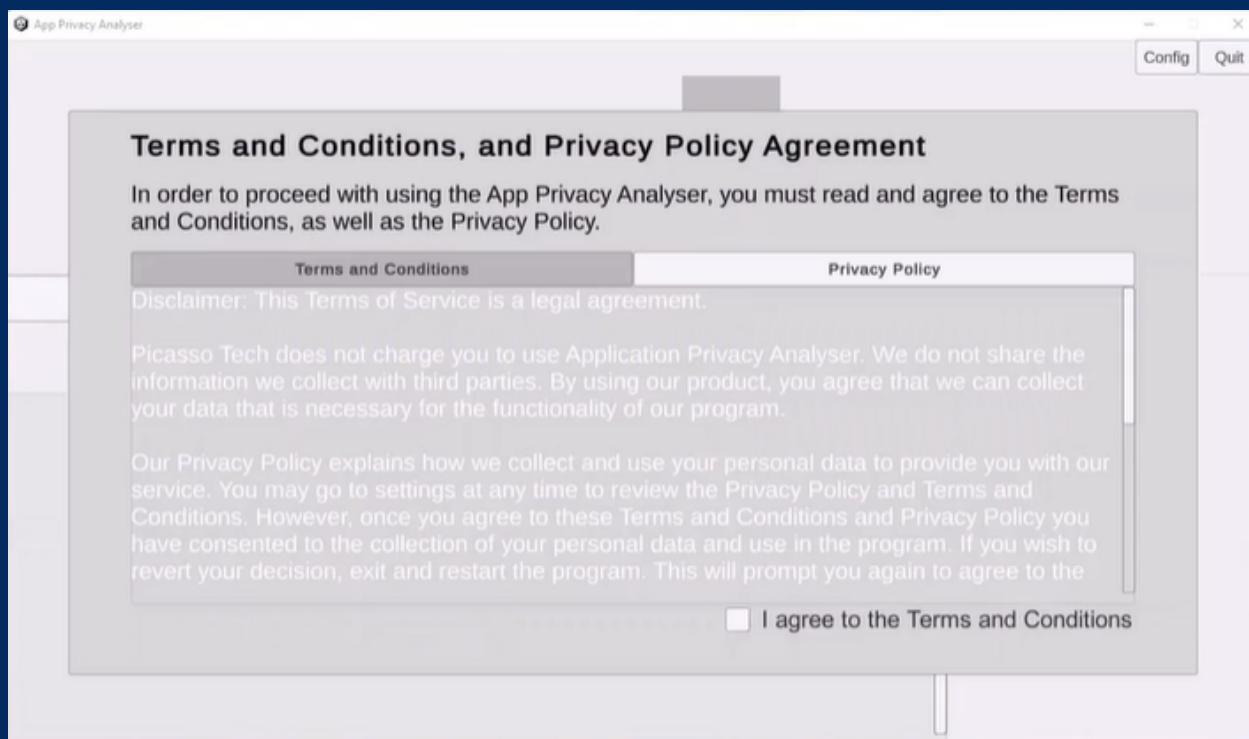
APPENDIX F - UML DIAGRAM



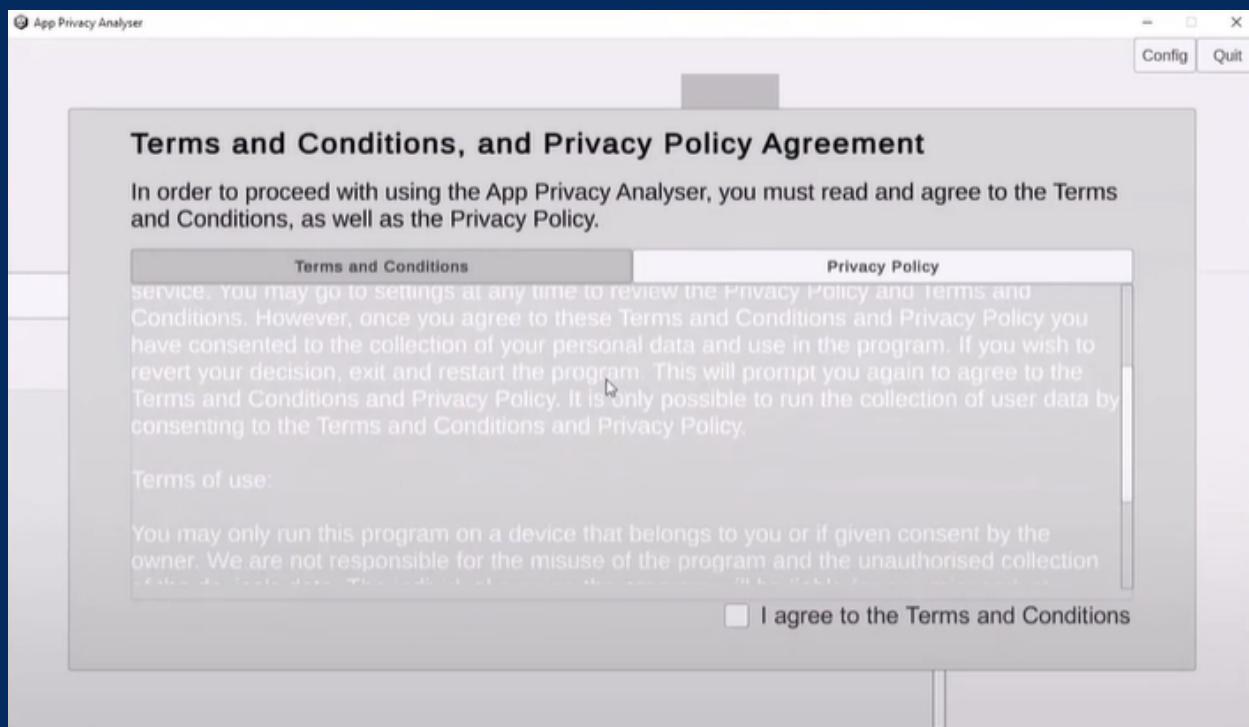
APPENDIX G - SYSTEM ARCHITECTURE



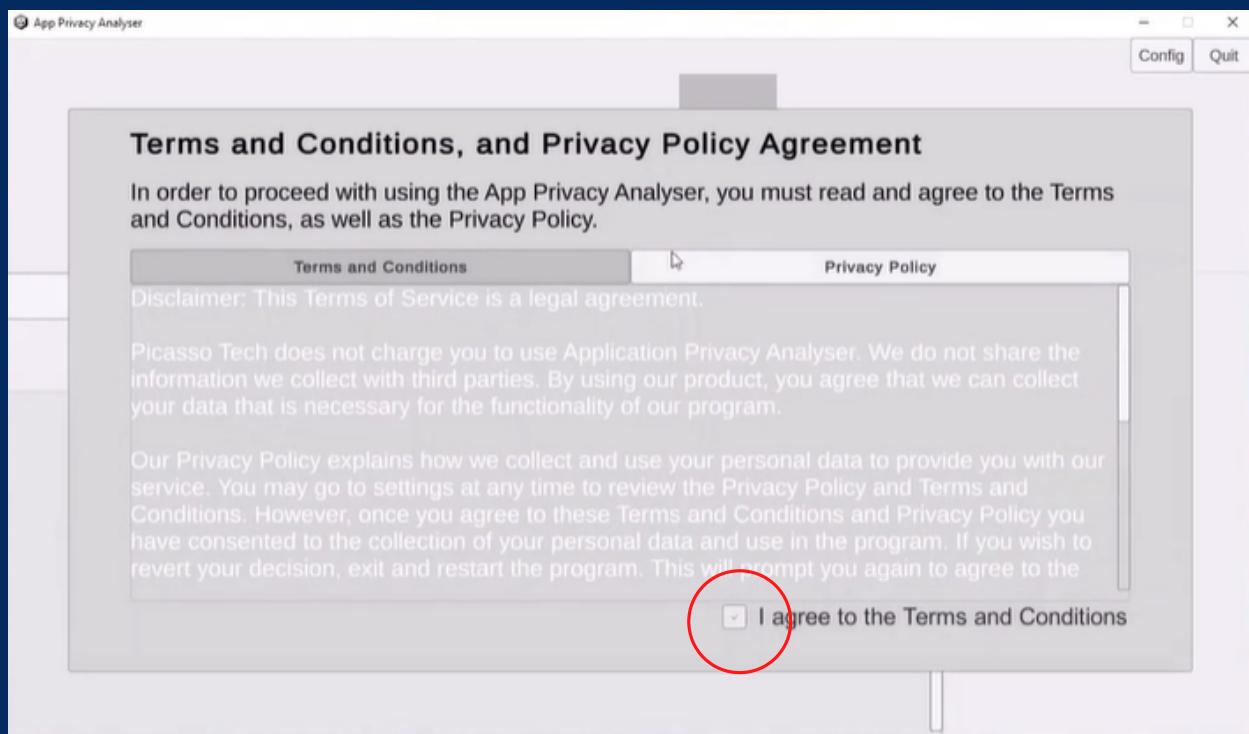
APPENDIX H - TERMS & CONDITIONS



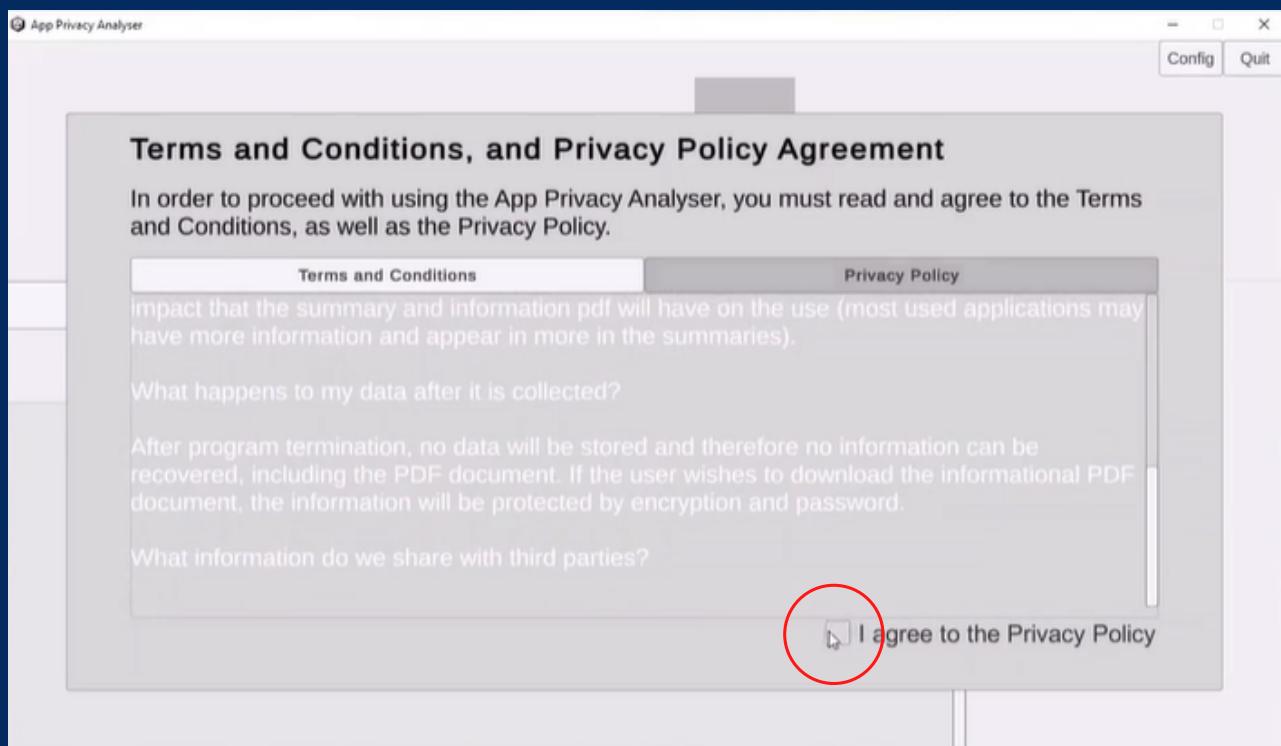
APPENDIX I - PRIVACY POLICY



APPENDIX J - TERMS & CONDITIONS CHECKBOX



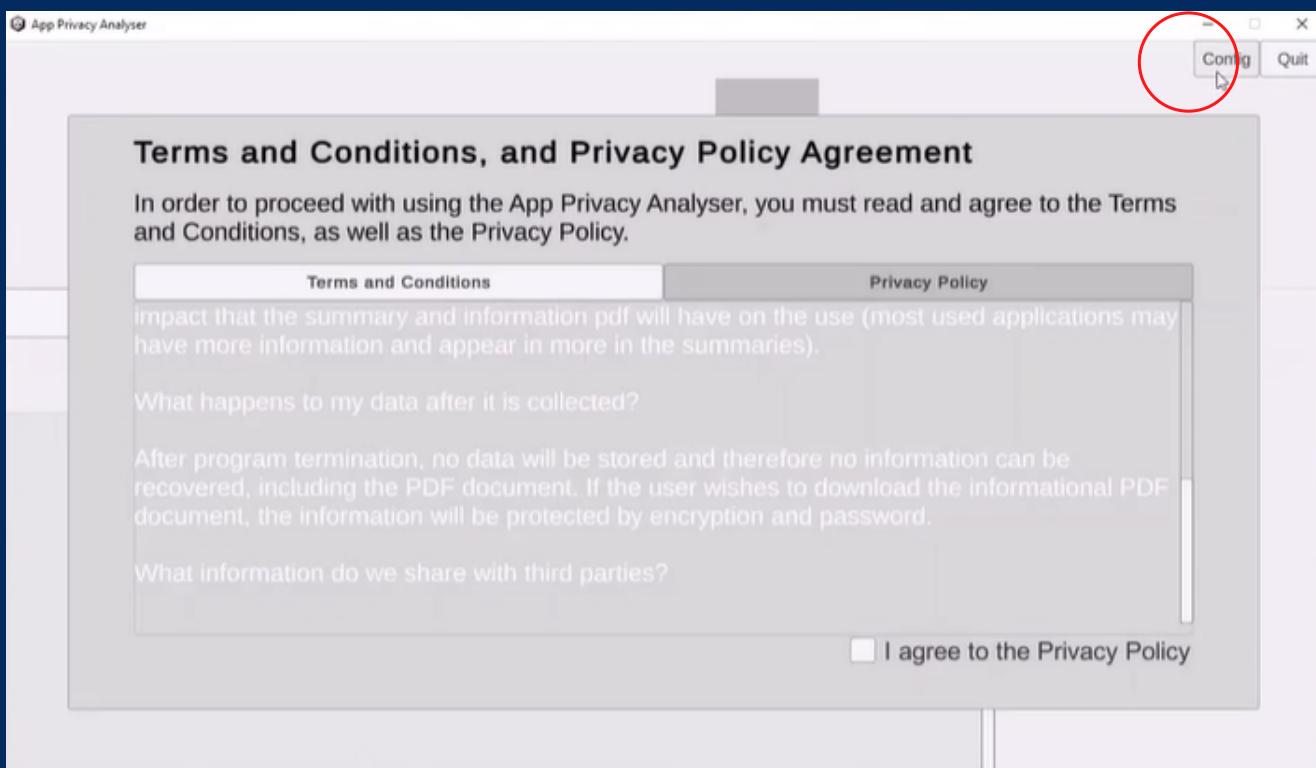
APPENDIX K - PRIVACY POLICY CHECKBOX



APPENDIX L - HOME SCREEN



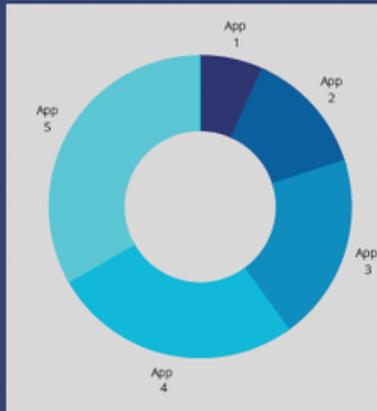
APPENDIX M - TERMS & CONDITIONS VIA CONFIG



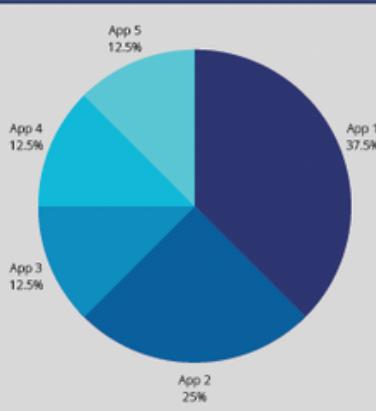
John Doe's Privacy Report

Device: iPhone 8

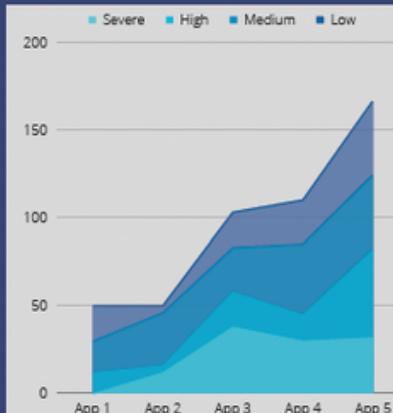
My Top 5 Data Collecting Apps



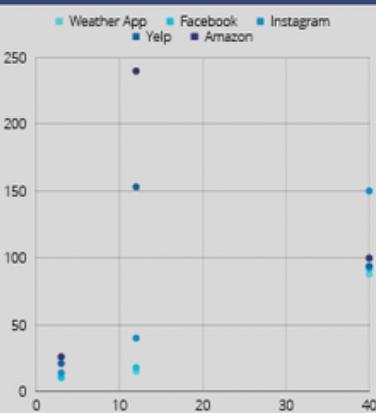
Most Data Used



Severity Levels



Location Usage



Device Summary

Device Summary Content

Device Summary Content

Device Summary Content

Device Summary Content

Device Summary Content

Device Summary Content

What Techniques Have Been Used to Assess my Applications Privacy?

Assessment Techniques Content

Assessment Techniques Content

Assessment Techniques Content

Application Privacy Analyser Process

It is critical to understand the concepts and principles of information security to ensure you know how and what data is being used.

Application Privacy Analyser is designed to look for privacy-related flaws such as a vulnerability or weakness that could jeopardise your mobile device's privacy. A detection technique is used and searches for previously identified faults or defect patterns.

User Guide:

My Top 5 Data Collecting Apps:

The five listed applications have been identified as the main applications that have been gathering your mobile device's data. A variation of data categories have been detected ranging from user ID and location data types.

Most Data Used:

The percentages allocated for your top 5 data collecting applications have been calculated and weighted accurately to reveal the application which uses the most of your data. Social media and entertainment based categories have been detected.

Severity Levels:

Severe: Significant warnings and potential data breaches found. It is advised to reconsider keeping the identified application(s) on your device.

High: High vulnerabilities found. It is advised to reconsider keeping the identified application(s) on your device.

Medium: Moderate and regular data collection processes found. Sensitive personal information is not at risk.

Low: Minimal data collection found. Sensitive personal information is not at risk.

Location Usage:

The applications that have been using your location data the most have been charted.

Information Security Basics

Learn More



Availability

Each letter within the CIA triad model represents a key principle in cybersecurity. The "CIA triad" is a commonly used standard for assessing the security of information systems. Learn more about this model on the next page!



John Doe's Privacy Report



Information Security Best Practices

How Do Applications Track Data?

“Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.”

Create and insert model here - visual representation of this process

Why Do Applications Track Data?

“Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat.

“Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.”

How Can I Protect my Data?

Here are some effective steps you can take now to begin securing your personal information and become #cyber-smart:

- Keep your mobile device up to date with the latest software version available. Generally, fixes for security gaps and vulnerabilities are provided within updates. Updated systems and security patches prevent the risk of data breaches from occurring.
- When installing a new application, it is vitally important to read, understand, and check the terms and conditions as well as the privacy policy. This is advised to refer to so that you are aware of what you are agreeing to when using the new application. Additionally, you can gather information about the data collection and management processes that are involved with the selected application.
- Avoid using public Wi-Fi networks when browsing the internet. Any time you decide to connect to another organisation’s network, your information and device is at risk of exposure to hackers and malware.
- Turn on your two-factor authentication settings. This method adds to the concept of passwords to develop a significantly more robust security solution. A password and information regarding something personal that you know are required to gain access to a network. The adoption of this additional security hurdle reduces the risk of unwanted users gaining access to your accounts and data.

- continued

CIA Triad Model

“Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat.”

“Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.”

“Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat.”

“Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.”

References

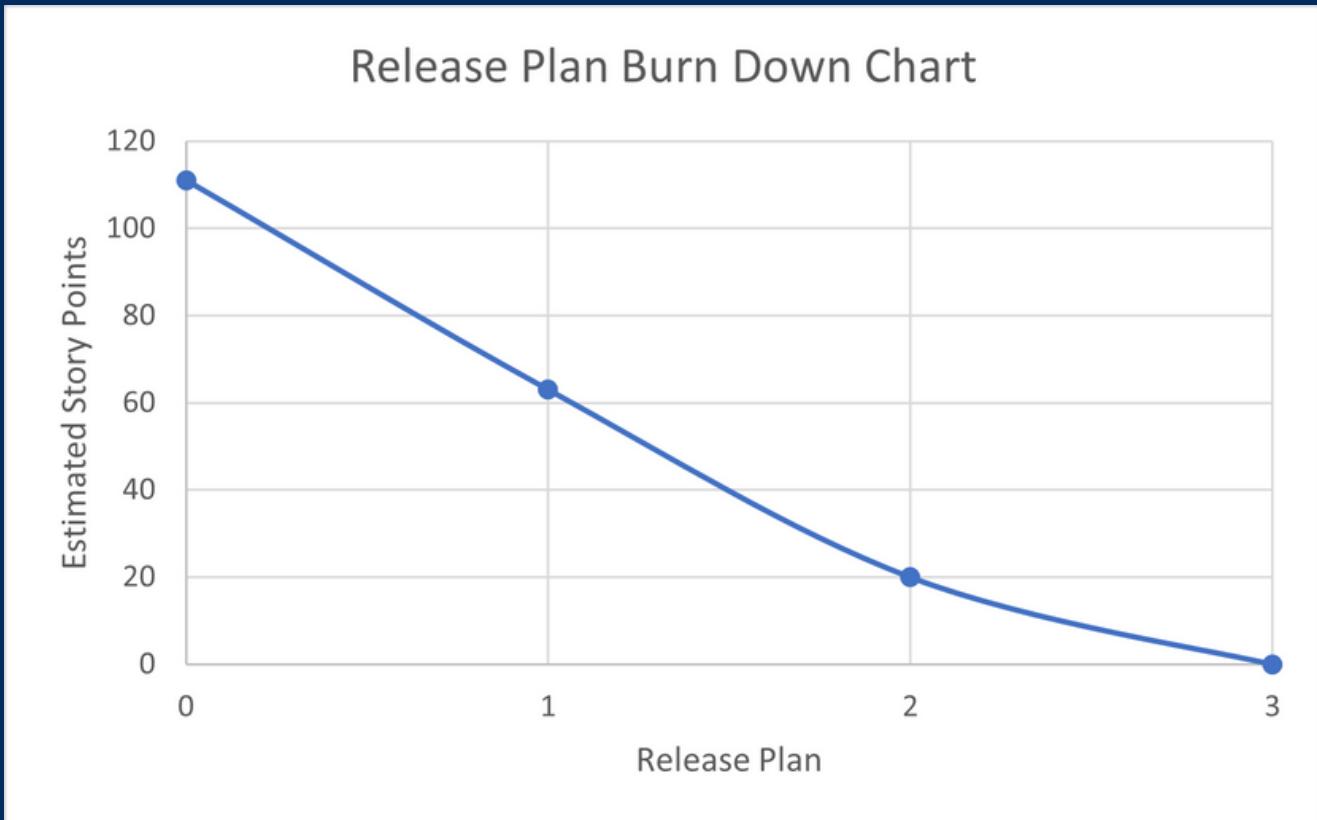
Fenrich, K. (2008, February). Securing your control system: the “CIA triad” is a widely used benchmark for evaluating information system security effectiveness. *Power Engineering*, 112(2), 44+. <https://link.gale.com/apps/doc/A17702877/AONE?u=anon-48d4c655&sid=googleScholar&id=1d03f795>

Watts, S. (2016). Secure authentication is the only solution for vulnerable public wifi. *Computer Fraud & Security*, 2016(1), 18-20.

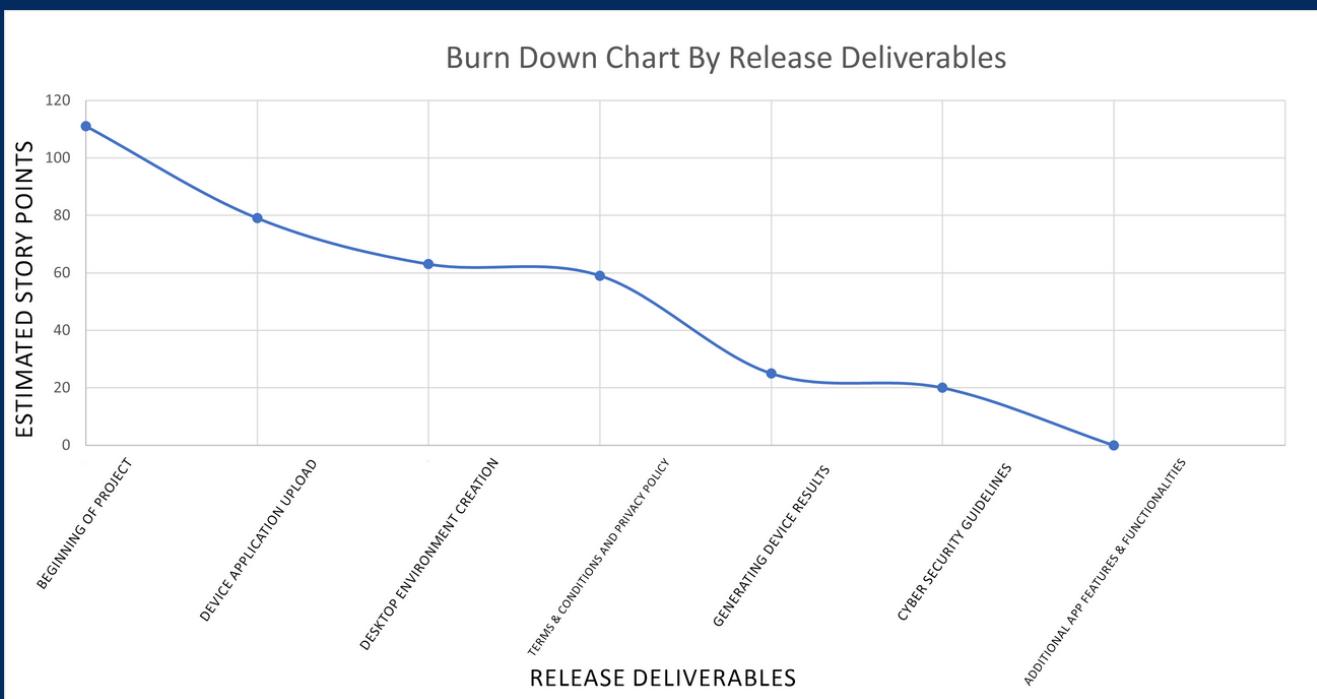
-continued



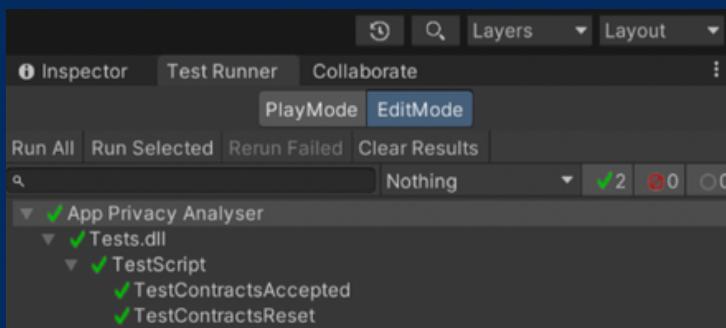
APPENDIX O - BURN DOWN CHART AS RELEASE PLANS



APPENDIX P - BURN DOWN CHART AS RELEASE DELIVERABLES



APPENDIX Q - UNIT TESTING



Unity's Test Runner running the two unit tests

```
// Test that when a user accepts the Privacy Policy and
// Terms and Conditions then the contracts menu disappears
[Test]
public void TestContractsAccepted()
{
    // Create test UI and contracts menu
    UIManager uiManager = new UIManager();
    GameObject contractsMenu = new GameObject();

    uiManager.contractPanel = contractsMenu;

    // Simulate user accepting both contracts
    uiManager.ToggleContract(0);
    uiManager.ToggleContract(1);

    // Check that the contracts menu is disabled
    Assert.AreEqual(contractsMenu.activeInHierarchy, false);
}
```

The unit test for ensuring correct functionality when a user accepts both contracts

APPENDIX R - CODE SNIPPET

```
// Booleans
private bool termsAndConditionsAccepted = false;
private bool privacyPolicyAccepted = false;

// Sets the initial menu to display the Terms and Conditions
public void TermsAndConditions()
{
    // Set button colours
    termsAndConditionsBtn.GetComponent<Image>().color = onBtnColor;
    privacyPolicyBtn.GetComponent<Image>().color = offBtnColor;

    // Update text content to the Terms and Conditions
    contentBox.GetComponent<TextMeshProUGUI>().text = textManager.termsAndConditionsText;

    // Display the Terms and Conditions toggle
    privacyPolicyTgl.SetActive(false);
    termsAndConditionsTgl.SetActive(true);
}
```

From Picasso Tech's UIManager class demonstrating code readability

APPENDIX S - RESEARCH REFERENCES

- Agarwal, R. (2022). 17 best iTunes alternatives you can use. Beebom. <https://beebom.com/best-itunes-alternatives>
- Apple Developer. (2022). Apple developer documentation. https://developer.apple.com/documentation/devicemanagement/list_the_installed_apps
- Bellairs, R. (2019). What is code quality? Overview + how to improve code quality. Perforce Software. <https://www.perforce.com/blog/sca/what-code-quality-overview-how-improve-code-quality>
- Clarke, R. (2014). Privacy and social media: An analytical framework. *Journal of Law, Information and Science*, 23(1), 169-191.
- Codegrip. (2020). Why is code quality important?. <https://www.codegrip.tech/productivity/why-is-code-quality-important>
- Gibbons, S. (2018). What really happens when you allow a app to access your photos. ECHO. <https://www.liverpoolecho.co.uk/news/liverpool-news/what-really-happens-you-allow-15186255>
- Granwal, L. (2022). Australia - mobile OS share 2021. Statista. <https://www.statista.com/statistics/861532/australia-mobile-os-share>
- Haystack. (2017). About the ICSCI haystack project. <https://haystack.mobi/>
- Microsoft. (2021). C# coding conventions. <https://docs.microsoft.com/en-us/dotnet/csharp/fundamentals/coding-style/coding-conventions>
- Ostorlab. (2022). Mobile and web security testing automation augmented with exceptional attack surface discovery. <https://www.ostorlab.co/>
- Parasoft. (2022). What is code quality?. Parasoft. <https://www.parasoft.com/solutions/code-quality>
- Sealights. (2022). Code quality metrics: Is your code any good?. <https://www.sealights.io/code-quality/code-quality-metrics-is-your-code-any-good>

