FUNCTIONAL SPECIFICATION

eirguard

Cybersecurity governance and compliance

Peter O'Hare

Project Supervisor

Dr. Christopher Staff

Table of Contents

Introduction *2*

ENISA Threat Landscape 2023 2

Questionnaire 3

eirguard *4*

Project Scope *5*

Technology Considerations *5*

Android 5

Hosting & Deployment 6

Competitors and Similar Applications *6*

System Overview *7*

Functional Requirements & FURPS *8*

Core requirements: 8

App: 8

Website: 8

Supabase 8

FURPS+ 8

Metrics *10*

Gantt Chart 10

Use Case / Misuse Case Diagram *11*

User Flow Diagrams *12*

User login process 12

User login security flow 12

Technical Requirements *14*

Software 14

Hardware 14

Platforms Utilised 14

References *15*

Introduction

Cybersecurity is an important consideration for any business in 2023. Ignoring cybersecurity means putting the business severely at risk, or indeed putting the customers or clients of the business at risk.

According to the UK's *Cyber Security Breaches Survey 2022*,[1] 39% of respondents who identified an attack, stated the most common threat vector was phishing. However, 21% reported a more sophisticated attack such as denial of service, malware, or ransomware attacks.

Within the groups reporting attacks 31% of businesses and 26% of charities reported they were facing an attack at least once a week. One in five of those businesses and charities stated they had suffered a negative outcome because of those attacks.

ENISA Threat Landscape 2023

The ENISA Threat Landscape report 2023 [2] identified the top 5 cybersecurity threats as:

I. Ransomware
II. Malware
III. Social Engineering
IV. Threats against data
V. Threats against availability (ddos)

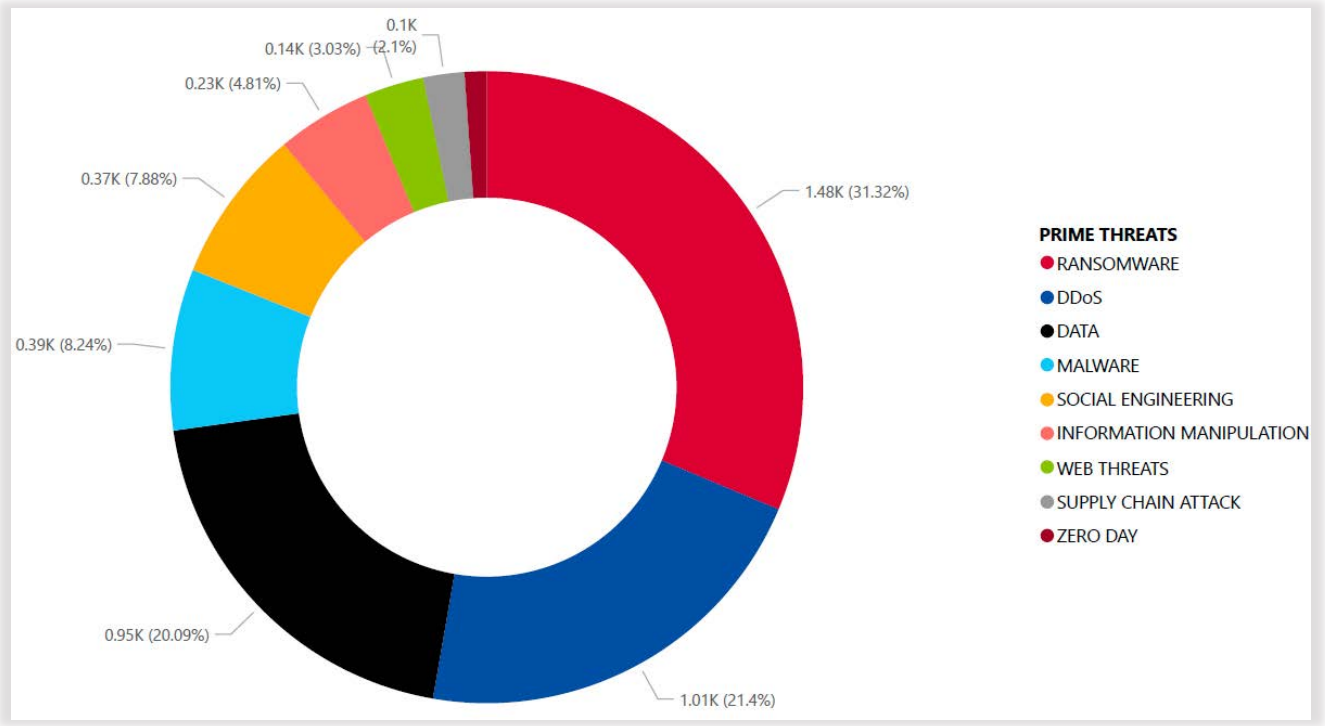


Figure 1: ENISA Threat Landscape 2023 Threats

The ETL 2023 report also investigated the motivations behind the attacks and discovered that financial gain was by far the biggest motivator.

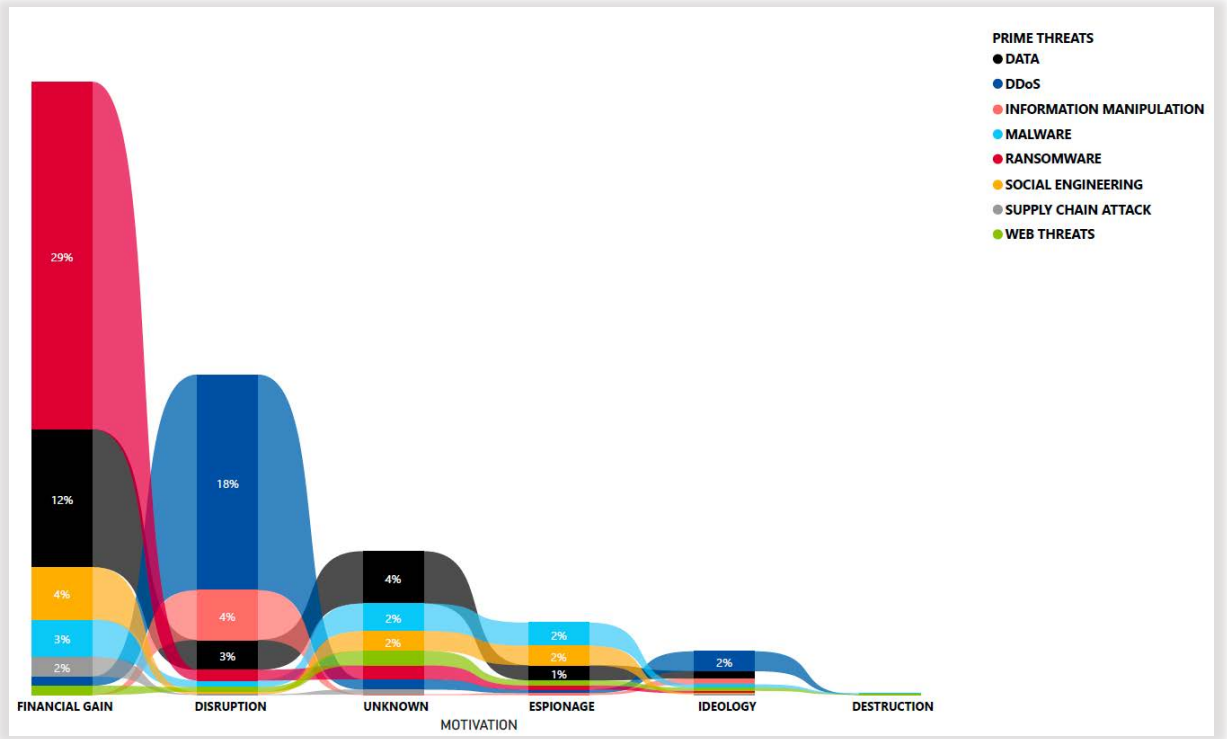


Figure 2: Motivating factors for cyber attacks

With the EU NIS2 cybersecurity regulations coming into effect in October 2024, the broader scope of the new regulations means that businesses who fall under the new category of "**Important**" - or indeed supply services to a business who is designated as Important – will now have to comply with the regulations in full.

Questionnaire

As part of my research, I created a cybersecurity awareness questionnaire (available here)[1] and asked representatives from five companies if they could participate. At the time of writing, I had received one completed response.

The response can be distilled as follows:

- less than 50 employees on site
- some cybersecurity policies in place
- not following a particular cybersecurity framework
- no dedicated cybersecurity officer on site
- management reviews of cybersecurity policies are in place
- company needs to comply with the incoming NIS2 regulations
- company is developing an in-house strategy for compliance
- good at reviewing current policies, software & hardware inventories, and critical assets
- not so good with staff awareness training, or disaster recovery policies
- organisational risk appetite also unknown

[1] https://forms.office.com/e/igzc5peGi6

The above example could conceivably be applied to numerous organisations of a similar nature throughout Ireland, and indeed beyond. While some areas identified are quite good, others are severely lacking. This deficit could be attributed to several factors - budget constraints, staffing issues, a lack of knowledge, complacency, laziness, or plain old neglect. The fact remains however, that there are large gaps in basic cybersecurity hygiene.

If we extrapolate these assumptions out to incorporate similar sized organisations throughout the country – we expose quite a large problem in cybersecurity hygiene as a whole – not to mention possible issues attaining NIS2 compliance.

If only there was a comprehensive, straightforward, intuitive, informative, cost effective, and efficient way of solving these issues…

eirguard

Eirguard is an iPadOs application, with an online administration portal, that aims to make cybersecurity compliance easier, less cumbersome and more cost effective for small and medium sized enterprises.

Eirguard will take a snapshot of an organisations current cybersecurity stance, ascertain their ultimate aims and goals, and assist in the creation and monitoring of an action plan to achieve those goals. As part of the onboarding process eirguard will also ascertain any legal or regulatory obligations that need to be adhered to and build those into the plan.

Eirguard can be used by a single individual to complete the process, or by a team in larger organisations. An administrator or project lead can create users and roles and assign tasks to individual users for completion. Completed tasks are then fed back to the admin dashboard on the web portal, where progress can be monitored, reports created and shared, or policy reviews scheduled for future dates.

Eirguard will draw from the upcoming CSF2 (Cybersecurity Framework 2) currently undergoing review, as well as NIS2 requirements (also still under review) as well as industry best practice to achieve both the clients' stated goals, and regulatory compliance goals.

Project Scope

Eirguard is targeted at small and medium sized enterprises who wish to take full control of their cybersecurity management and deployment. It will focus on removing the barrier to compliance that can be put in place by sometimes vague and complex language, or difficult to grasp criteria. Eirguard intends to level the cybersecurity compliance playing field by ensuring that all businesses can protect themselves, and their clients or customers from a cyber-attack.

Eirguard is positioned to be used by both technical and non-technical users. While some knowledge of cybersecurity would certainly be an advantage, eirguard should not be a challenge for the general user, as explanations and tutorials will guide them through each stage of the process.

The ultimate outcome for an organisation using eirguard should be the creation of a robust cybersecurity action plan, as well as a mechanism for influencing the organisation's approach to cybersecurity governance, incident handling, and progress monitoring moving forward.

Technology Considerations

Various options for build technology and platforms were considered at the beginning of the planning process. This section will look at some of those alternatives.

Android

Android has a larger user and install base than iOS, as well as significant market penetration with numerous manufacturers such as Samsung, Google, Xiaomi, Nokia, Doro, Honor etc. Despite this large user base, the decision ultimately was made to go with iOS.

The Android device market is extremely fragmented, with many competing manufacturers supporting different screen densities, sizes, and technologies. Samsung themselves have tens of differing models in their line-up from high to low end devices, as well as foldables. This meant supporting many different device specifications, sizes, and capabilities if the project was to move forward with Android.

The other main consideration was tablet apps on Android are not really considered by developers at present, despite the fact many manufacturers make Android tablets. This means there's a dearth of tablet specific developer resources available.

Therefore, iOS was chosen as the app platform because:

- Standardised screen sizes and resolutions across the device range
- Ease of code reuse between iPadOS & iOS using SwiftUI
- Developer resources available for both iOS and iPadOS

Hosting & Deployment

Firebase seems to be the industry standard when deploying an application, and for good reason. It has built in analytics, powerful features and the might of Google behind it.
However, Google is notorious for killing services with very little reasoning, meaning one cannot truly depend on any platform it offers. This website tracks such killed services: Killed by Google. [2]

Firebase, while offering some desired functionality, did not offer everything required, like ease of encryption and user authentication. It also had the potential of getting expensive very quickly once the free tier was exceeded. Hosting is confined to Google's own cloud services, which again adds to ever rising costs, and is quite restrictive. The cons far outweighed the pros with Firebase, regarding possible changes Google might make, including pricing, services and the general uncertainty of the platform.

Amazon Web Services (AWS) was also considered but ultimately not chosen because of the high cost of the differing services required, and the relative complexity involved in utilising and integrating them into the application.

Competitors and Similar Applications

At present a search of the iOS App Store returns only one app that closely resembles eirguard. CyberSmart is a UK based company helping with documentation, training, and active device monitoring. It doesn't however, address cybersecurity governance or policy creation. Any other cybersecurity app returned, seemed to relate to VPN's, device monitoring, news, or learning.

In Ireland, large organisations like Grant Thornton, EY, Nostra and Security Risk Advisors will assist in cyber security audits, governance, and compliance. However, none of these offer a stand-alone application or tool, rather a security audit - with a view to a continuing contract for active monitoring of the network.

Examples of online platforms that offer compliance and governance assistance are Drata, ControlMap, and HyperProof. These platforms have a range of compliance frameworks to choose from, including GDPR, NIST and ISO27001, to name but a few.

They do not however offer a stand-alone application, instead offing a web only dashboard. All three will conduct a cybersecurity audit of an organisation, with only Drata giving approximate pricing for the service. This is listed as between €7,000 and €14,000 for a snapshot of current security controls only. Should the organisation require a deeper audit and suggestions for improvement – pricing goes from €12,000 to €20,0000. There is of course a massive upsell and push by each platform towards their own range of 24/365 monitoring services.

[2] https://killedbygoogle.com

System Overview

eirguard will consist of a native iOS app – mainly targeting iPadOS - written in Swift. The app itself will handle the bulk of user interactions while conducting audits, carrying out action plans, or any "field" work.

As well as for the reasons outlined in the *Technology Considerations* section, iOS was also chosen as a development platform because of the iPad's market share. Between 2020 and Q2 of 2023 iPad's market share was at 54.7% and showing no sign of declining.[3] Apple's App Store is vigorously vetted and much more secure than Google's Play Store.[4]

Apple pushes software updates for iOS on a regular basis, making iPadOS more secure when compared to Android devices, which can sometimes wait months for security updates to be pushed by the various manufacturers.

Apple's iOS and iPadOS developer documentation is easy to find, well documented and explained, and makes for an invaluable companion for development.

eirguard will also have a web-based administration dashboard, where roles, permissions and tasks can be managed by the project lead. Here, progress can be tracked, and reports generated and shared with management or other stakeholders.

The administration website will be built using the Django web framework. This has significant advantages as Django is robust, mature, well supported and documented. It's also secure out of the box, as it enables protection against many web vulnerabilities by default, including SQL injection, cross-site scripting, cross-site request forgery and clickjacking. [5]

Both the app and the administration site will utilise Supabase[3] for database support. Supabase is an open source Firebase alternative, utilising a Postgres database. Out of the box, Supabase offers many features as standard that Firebase does not. These include data encryption, user authentication, and a fully featured "views" mechanism that allows for custom views to be created on the fly without the need for foreign keys. This allows for greater control over how the data is accessed, how the data is stored, implementing encryption, and controlling user authentication.

Throughout the design and development process, the security by design doctrine will be closely adhered to. This will help identify and mitigate potential security issues before they arise, and demonstrate adherence to a security first approach to the development process.

[3] https://supabase.com

Functional Requirements & FURPS

Core requirements:

App:

The iOS app must allow for users to sign in and undertake whatever task has been assigned to them, or in the case of a single user – allow them to initiate an audit and develop an action plan.

The app must provide as much feedback to the user as possible while completing tasks. This can be achieved utilising ui elements, visual cues, and/or a checklist. It is imperative that the user understands where they are in the process of their current task.

Website:

The administration dashboard must communicate progress clearly and efficiently.
The user management section should be intuitive and straightforward, with role based access provisions, to provide users with only the access they require to complete their tasks. Report generation on progress to date should be implemented to enable the sharing of progress with management.

Supabase

Connection to the database must be encrypted using ssl.
User management: roles and permissions must be managed easily & efficiently.
Encryption: all usernames & passwords must be encrypted. As organisations will be storing information on their cybersecurity makeup, all user data provided by them must also be encrypted. Redundancy: regular backups must be taken to ensure availability in the event of an incident.

FURPS+

Functionality	
Policy Development	The app must assist organisations in developing and maintaining comprehensive cybersecurity governance policies
Regulatory Compliance	Provide guidance and templates to help organisations meet relevant cybersecurity regulations (e.g., GDPR, NIS2, DORA).
Documentation Management	Allow organisations to manage and store their cybersecurity policies and related documents securely
Audit Trail	Maintain an audit trail of policy changes and user activity to ensure accountability.

Usability	
User Interface	Design an intuitive and user-friendly interface, making policy creation and management straightforward for users with varying levels of expertise
Educational Resources	Include educational materials and best practices to aid organisations in understanding and implementing cybersecurity governance
Customisation	Permit organisations to tailor policies to their unique requirements and industry specifics

Reliability	
Stability	Ensure the app's stability, reducing the risk of data loss, crashes, or interruptions in service
Data Integrity	Implement safeguards to protect the integrity of stored policies and documentation.
Regular Updates	Provide consistent updates to adapt to changing regulations and security best practices

Performance	
Efficiency	Optimise the app for responsive performance without taxing the iPad
Scalability	Design the app to handle growing volumes of policies and documentation as organisations expand
Resource Efficiency	Ensure the app uses system resources efficiently, preserving battery life and memory

Supportability	
Customer Support	Offer accessible channels for customer support to address questions and issues
Documentation	Maintain updated documentation for both end-users and administrators
Integration	Ensure compatibility with other organisational software and services to facilitate a holistic approach to governance

In addition to the FURPS laid out previously, the following areas also need to be considered:

Assumptions	
Assumption 1	Organisations have a basic understanding of the iPad and iOS platform
Assumption 2	Organisations are motivated to develop and maintain effective cybersecurity governance policies
Assumption 3	The app's guidance will align with specific industry and regulatory requirements.

Risks	
Risk 1	Rapidly changing regulations may necessitate continuous updates to the app's guidance and templates
Risk 2	Inadequate governance policies could expose organisations to security risks and regulatory penalties
Risk 3	Scalability challenges may arise as organisations generate more policies and documentation

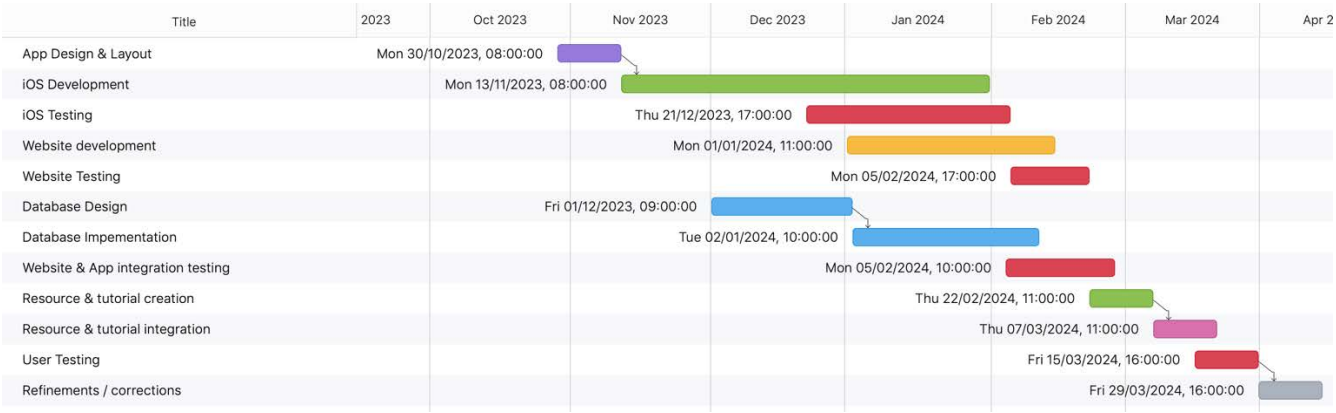
Metrics

The relative success of the project will ultimately come from testers, and those working in SME's who use and test the app to provide feedback. If the feedback is generally positive, and genuine interest is shown in the future of the app – then one could conclude that the endeavour was successful.

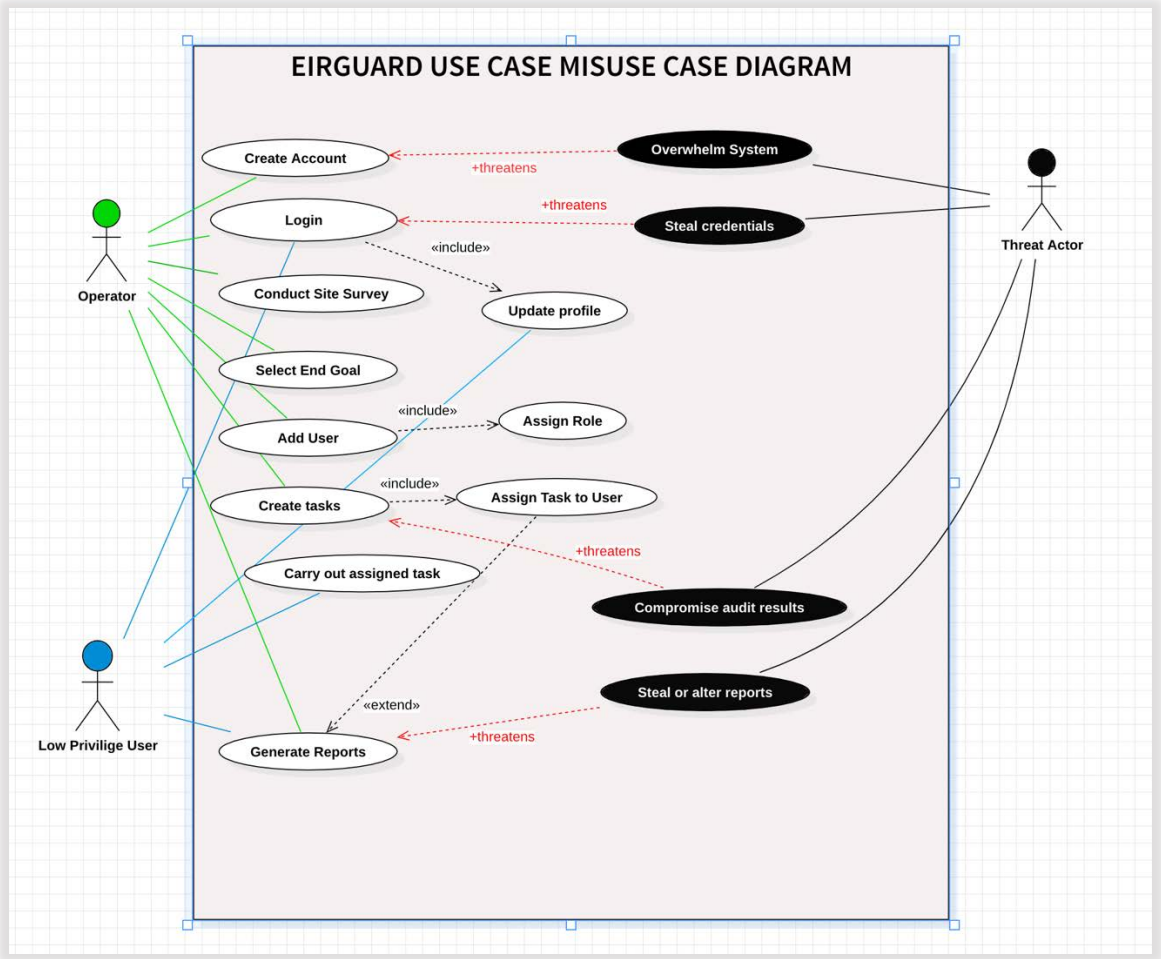
However, if feedback is not positive, and testers report difficulties using it, or cite unclear direction, confusing interfaces, non-functional features, or highlight other issues, then one can conclude that the goal of the project was not achieved and could be deemed a failure.

Gantt Chart

The proposed timeline outlined in the Gantt chart is approximate and assumes no unforeseen issues impacting development. This timeline can be revisited to account for overruns should any occur, and a review of the schedule can be carried out accordingly.



Use Case / Misuse Case Diagram



User Flow Diagrams

User login process

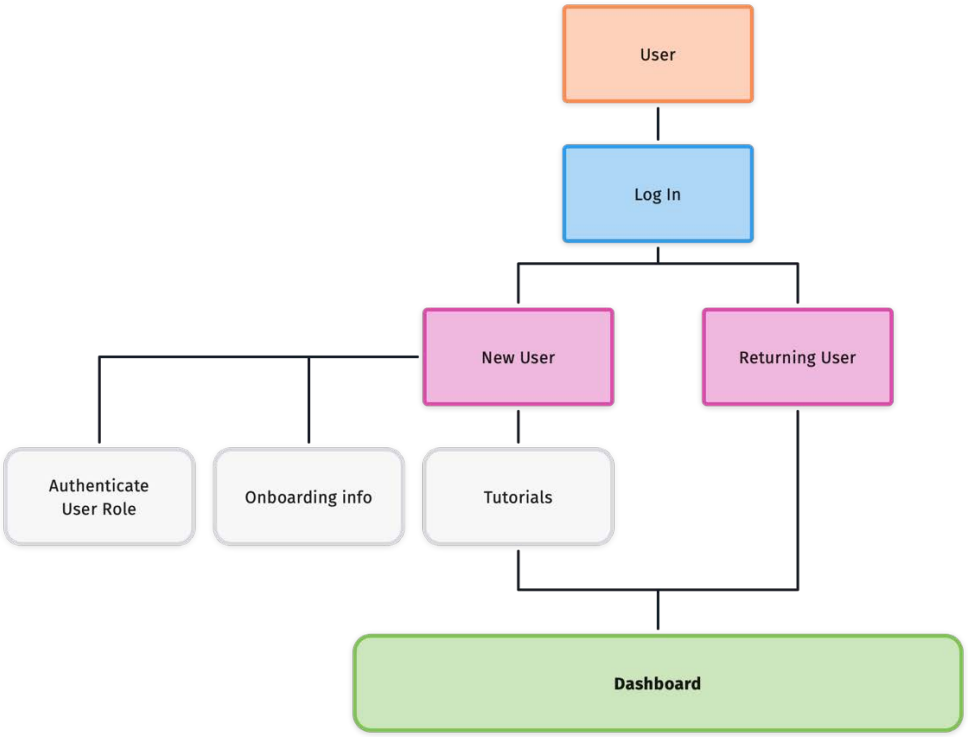


Figure 3: User login flow

User login security flow

Sample Screen Wireframes

Figure 4: Login Screen

Figure 5: Onboarding screen

Technical Requirements

Software

Software Requirements	
Xcode	Required to code & build the native iOS application
PyCharm	Required to code and work with the Python Django web framework
Git	Version control

Hardware

Hardware Requirements	
MacBook	Required to run Xcode to develop iOS application
iPad	Required to run & test application on device

Platforms Utilised

Platform Requirements	
Supabase	Open-source alternative to Google Firebase for deployment
Hetzner	Low-cost EU based shared VPS server to host Django site
Github	Repository for project code

References

[1] ‘Cyber Security Breaches Survey 2022 - GOV.UK’. Accessed: Oct. 17, 2023. [Online]. Available: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022#key-findings

[2] ‘ENISA Threat Landscape 2023 — ENISA’. Accessed: Oct. 20, 2023. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

[3] ‘Tablet Operating System Market Share Worldwide | Statcounter Global Stats’. Accessed: Oct. 22, 2023. [Online]. Available: https://gs.statcounter.com/os-market-share/tablet/worldwide/#monthly-202009-202309-bar

[4] ‘How cybercriminals evade mobile app store security measures | Security Info Watch’. Accessed: Oct. 26, 2023. [Online]. Available: https://www.securityinfowatch.com/cybersecurity/information-security/anti-virus-and-malware-defense/article/53074932/how-cybercriminals-evade-mobile-app-store-security-measures

[5] ‘Django introduction - Learn web development | MDN’. Accessed: Oct. 17, 2023. [Online]. Available: https://developer.mozilla.org/en-US/docs/Learn/Server-side/Django/Introduction