**STRUCTURED APPLICATION**

Table of Contents

[**Hybrid Methodology and Justification** 2](#_Toc189349734)

[Mobile Banking app 2](#_Toc189349735)

[Diagrams of Scrum and Agile methodology 2](#_Toc189349736)

[Justification for Scrum – Agile hybrid methodology 6](#_Toc189349737)

[AI Chatbot 7](#_Toc189349738)

[Diagrams of CRISP-DM and HCAI methodology 7](#_Toc189349739)

[Justification for CRISP-DM and HCAI hybrid methodology 12](#_Toc189349740)

[RPA System 12](#_Toc189349741)

[Diagrams of DevSecOps – Lean Six Sigma methodology 12](#_Toc189349742)

[Justification for DevSecOps and Lean Six Sigma hybrid methodology 12](#_Toc189349743)

[**Security Strategies** 12](#_Toc189349744)

[Mobile App 12](#_Toc189349745)

[AI chatbot 12](#_Toc189349746)

[RPA System 13](#_Toc189349747)

[**Sustainability and Green IT** 14](#_Toc189349748)

[General Guidelines for all projects 14](#_Toc189349749)

[AI Chatbot 14](#_Toc189349750)

[Mobile App 14](#_Toc189349751)

[RPA System 14](#_Toc189349752)

[**Multi-tenant Architecture design for AI Chabot** 14](#_Toc189349753)

[**Risk Management** 14](#_Toc189349754)

[Risk Management Diagram 14](#_Toc189349755)

[Risk Management Plan Explanation 14](#_Toc189349756)

[Risk Committee 14](#_Toc189349757)

[**References** 14](#_Toc189349758)

# **Hybrid Methodology and Justification**

## Mobile Banking app

### Diagrams of Scrum and Agile methodology

|  |
| --- |
| A white board with papers on it  Description automatically generated |
| *Entire Agile – Scrum Methodology Diagram A* |

|  |
| --- |
| A white board with writing on it  Description automatically generated |
| Agile – Scrum Methodology Diagram A.1 |

|  |
| --- |
| A white board with writing on it  Description automatically generated |
| Agile – Scrum Methodology Diagram A.2 |

|  |
| --- |
| *A close-up of a paper  Description automatically generated* |
| *Agile – Scrum Methodology Diagram A.3* |

### Justification for Scrum – Agile hybrid methodology

This hybrid methodology allows consistent clarity of tenable short-term goals. Goals that have been carefully prioritized to maximize stakeholder satisfaction, with the ability to prepare the next cycle with possible improvements to further increase development efficiency. For a Mobile app that handles crucial functions it is important to be prepared for quick responses to stakeholder requests and minimise risk to the system during implementation.

This also allows repetitive SAST and DAST security checks during the Execution phase in every Agile cycle. Additionally, compliance to the DPA 2018 and ISO 27001 standards can be reviewed and set during the planning meeting before the sprint begins. Such as the principles of the DPA **2. (Data Protection Act 2018, no Date)** Chapter 2 Principles: Section 86 to 91.

Due to its constant team meetings before and during the sprint, this allows for reviewing past performance to improve and the ability for flexibility. To amend the plan during short notice for optimal results and allow the team to amend the scale of projects and tasks for the next update.

Due to the system being a mobile app, the storage systems can be set up in a scalable environment. Such as the cloud.

Efficiency is increased by the autonomy this method provides to its workforce. It keeps direct and constant communication between staff, with clear designated teams. Allowing a workspace of high levels of collaboration and individualism.

After the agile cycle, and once the completed component has been integrated, the team can review their performance throughout the cycle and plan for the next cycle retrospectively.

Risk is reduced by implementing small increments to the final project. Meaning if one of these updates has a fault, the negative affect on the final product is minimized.

## AI Chatbot

### Diagrams of CRISP-DM and HCAI methodology

|  |
| --- |
| A white board with writing on it  Description automatically generated |
| CRISP-DM & HCAI Diagram A |

|  |
| --- |
| A diagram of a business strategy  Description automatically generated with medium confidence |
| CRISP-DM & HCAI Diagram B.1 |

|  |
| --- |
| A white board with writing on it  Description automatically generated |
| CRISP-DM & HCAI Diagram B.2 |

|  |
| --- |
| A white board with writing on it  Description automatically generated |
| CRISP-DM & HCAI Diagram B.3 |

|  |
| --- |
|  |
| CRISP-DM & HCAI Diagram C |

### Justification for CRISP-DM and HCAI hybrid methodology

This diagram allows a well-defined framework for data mining and ethical compliance during the process. With data driven goals and objectives, it allows the iterative process to respond effectively and provide sufficient results at the end of the cycle to all stakeholders. Along with constant monitoring of ethical and legal compliance during the development process. This is crucial for the development of an AI system due to the growing public awareness of these systems.

Data security is a priority, and with the hybrid methodology providing numerous functions to ensure the safety of the data subject. Functions such as encryption and anonymising (CRISP-DM) , testing in a live scenario and documenting all data utilized ( HACI ) Will help maintain legal and ethical standards from the ISO 27001, such as:

* **3.(Secfix.com, 2024)**” ensures that personal data and other sensitive information used by AI systems are properly handled, processed, stored, and disposed of.”

Additionally, due to the cycle being data driven; customer experience is deeply integrated in the decision-making process. Aswell as optimizing cost and time, for the goals of the cycle will be accurate and clearly defined.

Risk will be minimized since the AI will be trained by up-to-date datasets, as well as ran through accurate scenarios it may encounter once live. Therefore, latency errors, crashes or downtime can be identified during the development section.

ESG standards can be followed by implementing methods such as:

* Optimising the AIs source code to reduce computational power requirements.
* Full transparency of the data the AI uses, as well as the reasons for the use.
* Clear and constant user rights. Such as opting out of the dataset

## RPA System

### Diagrams of DevSecOps – Lean Six Sigma methodology

|  |
| --- |
| A white board with writing on it  Description automatically generated |
| *Entire DevSecOps – Lean Six Sigma Methodology Diagram A* |

|  |
| --- |
| A white board with writing on it  Description automatically generated |
| *Entire DevSecOps – Lean Six Sigma Methodology Diagram B.1* |

|  |
| --- |
| A white board with red writing on it  Description automatically generated |
| *Entire DevSecOps – Lean Six Sigma Methodology Diagram B.2* |

|  |
| --- |
| A white board with writing on it  Description automatically generated |
| *Entire DevSecOps – Lean Six Sigma Methodology Diagram B.3* |

|  |
| --- |
| A white board with a green button  Description automatically generated |
| *Entire DevSecOps – Lean Six Sigma Methodology Diagram B.4* |

|  |
| --- |
| A diagram of a diagram  Description automatically generated with medium confidence |
| *Entire DevSecOps – Lean Six Sigma Methodology Diagram C* |

### Justification for DevSecOps and Lean Six Sigma hybrid methodology

This hybrid methodology allows smooth roll out of updates with minimal impact on the live system which will be essential for the day-to-day functioning of the company. If this backend processes are interrupted for any amount of time, it may have significant negative impacts. while allowing continuous monitoring of potential improvements for the next cycle. The L6S (Lean six Sigma) allows the development team to utilize user feedback during the process which enable more accurate cycle goals and stakeholder requirements to be met more efficiently.

Due to the system having automated decision-making, the DPA 2018 mut be adhered to. Such as

* **2. (Data Protection Act 2018, no Date) “**The controller must as soon as reasonably practicably notify the data subject that such a decision has been made.” If made using the automated process. This can stem from customers to internal staff in the company

The implementation of the L6S method provides multiple functions for monitoring and analysing the systems effectiveness. Such as Fishbone diagrams, a visual tool to identify the root cause of problems. This mitigates risk of allowing bugs to be implemented in the live version and improving time efficiency for the development team. Additionally, once the product has been released it can be monitored in real time. Using tools such as dashboards, further allowing potential improvements to be identified.

A phase of developing an improvement plan before release can be enacted, this is good practice to review and amend clear and accessible procedures for development and release. Improving the smoothness of releasing the update, increasing efficiency and cost.

Due to the ability for continuous improvement plans increase scalability and the performance enhancement.

# **Security Strategies**

The two main aspects that will be considered in in this section are integrating Quantum Resilient Security and Supply Chain Security. Due to traditional encryption is becoming increasingly insufficient due to more advanced quantum applications being more common. There are general guidelines that should be followed for all three applications, while more specific (and crucial) mechanisms for each application will be outlined.

### General guidelines to follow

* The guidelines from the National Institute of Standards and Technology (NIST) should be valued and followed. They provide a CSF (Cybersecurity Framework) that hold 6 key functions. Govern, Identify, Protect, Detect, Respond, Recover. **8. (National Institute of Standards and Technology, 2024)**
* All encryption methods must be PQC (Post Quantum Cryptography) algorithms.
* All third parties should be thorough vetted

### Vetting third parties

Any third-party software or applications that are implemented into our applications should be examined to satisfy security requirements. This can include checking the third-parties source code, if it is not open source, a request for access to their source code should be sent. Though this may be denied, it is more suitable to check this before implementing. All documentation of updates and changes they have made should be used to verify. Additionally, tools such as Static and Dynamic code analysis should be ran identify potential vulnerabilities or program errors. Public reputation of the third party’s application should also be analysed before a choice is made.

Dependency management for third parties should be maintained, this includes keeping a list of all third parties that have been implemented, as well as the data they are able to access and handle, and what other parts of the system rely on this third-party operation.

## Mobile App

For the Area of the Mobile App, QRS applications are essential for securing the abundance of sensitive data. Also due to the multitude of devices that can access / the portability and ease of use of the devices that can access this application. This will focus on integration encryption methods into the mobile to withstand attacks by quantum apparatus to ensure the safe transfer and storage and transfer of data.

* Multi - Factor Authentication, this can range from requiring a password and onetime passcode, or a biometric signature (such as fingerprint or face recognition). These must implement post- quantum cryptography (PQC) algorithms, such as CRYSTALS-Dilithim or CRYSTALS-Kyber. The latter **1. (Nowsecure.com, 2023)** “NIST has approved … as the standard KEM “– Key Exchange Mechanism.
* Following Key exchanges, since mobile apps require on this function for session distribution, Quantum Key Distribution should be implemented.
* Encrypting all data, stored locally or by the cloud, using PQC encryption methods. Including all backups
* HTTPS, TLS and FTP are considered vulnerable to quantum computer attacks. They must be updated with PQC algorithms to secure all data being transferred.

Third parties that are popular and have a strong reputation of reliability should be recommended (such as Mastercard, Visa, SendGrid, Microsoft Azure).

## AI chatbot

The AI chatbot's security must be top priority as it handles financial data. Given its front-end exposure, it must be protected against quantum computational attacks during and post development. Additionally, when the project is being developed the sensitivity of the source code and training dataset cannot be overlooked. Strict security measures during and after development will ensure compliance with legal and ethical standards.

In general, all encryptions must utilise PQC (Post-Quantum Cryptography) Such as FALCON, which is one of the three encryption standards recommended by NIST. This includes the training dataset, any data collected and stored through user input and data the algorithm uses to provide answers to user queries.

The source code itself must also be protected and using algorithms – such as Classic McEilece – to secure the AI model long term. This algorithm is a well-known and a secure choice due to its long standing in the community. **4.(Mceliece.org, 2019)** “introduced in 1978 by McEilece”.

During the supply chain, there will be major risks that must be considered, and there are methods to mitigate these risks. Such as:

* Data Poisoning: misleading the AI model by malicious altering of the training dataset. Quantum computation can make these amendments much harder to identify.

Solution: Differential Privacy (anonymising the data to protect the data subject) and Certified Robustness Verification (Guarantees accurate outcomes even if the data is slighted amended). Aswell as secure databases with limited access to authorised users, and thorough documentation of all changes.

* Backdoor attacks: If third party components (such as pre-trained models) are used, they may be compromised to undisclosed functions, such as specific inputs to bypass security measures.

Solution: Adversarial Testing (to try and identify these functions before release), Live monitoring of all inputs / outputs to detect anomalies.

All third-party components must be thoroughly vetted. This includes:

* Research reviews of past incidents / performances and third-party experiences.
* Penetration testing. Conduct thorough security testing.
* Ethical and legal compliance is up to date by the third party.
* Ensure all data is free from unauthorized manipulation or unethical/unlawful bias.
* PQC is implemented into the third-party component.

## RPA System

The RPA system will function in the back end and not process front-end inputs from users directly. However, it will handle an abundance of information with various levels of sensitivity in the backend of the business. Resulting in a requirement of high security.

The most probable threats to the RPA system would be as follows:

* Data interception
* Supply chain attacks via third parties or over dependencies.
* Script manipulation – editing the code of the RPA system itself.

These can be protected against / avoided through Quantum Resilient Security (QRS) and supply chain security implementation.

Data interception can be avoided by enabling secure End-to-End encryption techniques (such as using lattice-based cryptography) for safe data exchanges in the RPA system. Two-factor authentication and minimal access for all users will further minimize unauthorized access.

Secure Code Signing methods allow the detection of editing the RPA scripts, providing proof whether the script is a legitimate original.

Vetting third parties for authenticity will decrease risk in the supply chain. Creating a list of all third parties used (a software bill of materials) will allow an overview of potential threats and security holes. Aswell as real-time monitoring during the development phase will mitigate risk in the supply chain.

# **Sustainability and Green IT**

Sustainability and Green IT in this context will refer to the concept and practice of designing and developing software that minimizes environmental impact during the project’s lifecycle. This will include reducing energy consumption and aim to use durable/recyclable technologies.

This will be important to consider for greater brand reputation and cost effectiveness. There are methods that enhance all three projects collectively, as well as methods tailored to each specific project.

## General Guidelines for all projects

* Optimise program scripts to reduce storage space and computing power required.
* Delete redundant data to reduce used storage space.
* Reduce API calls to lessen background processing.
* Continuous energy consumption monitoring for all services.

Any physical buildings (such as data centres or offices) should be built sustainably, and have clean energy apparatus installed where possible, such as Solar panels on the roofs and heat pumps. Additionally, no buildings sites should compromise an area of outstanding natural beauty (AONB) that is protected by the **6. (UK Government, 2020)** CROW Act 2000 (Countryside and Rights of Way).

## AI Chatbot

Referring to the possibility of using third-party components, such a pre-trained model, will aid in reducing computing power consumption. However, vetting and security risks must be considered.

The chatbot will be AI-heavy and act as an enterprise bot, therefore a net neutral cloud host should be recommended. Such as Microsoft Azure Bot Service, a suitable candidate for several reasons

* Contains sustainability calculations to measure the chatbots carbon footprint
* 5.(azure.microsoft.com, n.d.) Aims to use 100% renewable energy by the end of the year.
* Multiple AI services that are optimized for energy efficiency

Along with Azures security and scalability potential, this is a strong candidate for hosting the AI project.

Other potential options include AWS (Amazon web services) or Google cloud. If an alternative decision is made, all requirements stated previously should be met.

Additionally, outputs from the chatbot regarding sustainability should be encouraging further reduction of waste and greater consideration of renewable energy and technology.

## Mobile App

The project should be optimized to function more effectively on circular technology (hardware that is durable and recyclable, with minimal energy waste) to discourage waste products. Devices such as smart phones should be encouraged. The app should also co-operate with the phones operating system to provide real-time energy consumption monitoring. This allows higher customer consciousness on their carbon footprint.

Functions that can be implemented during development can improve battery efficiency while upholding good user experience.

* Minimalist user design will reduce CPU and GPU usage. Avoid redundant animations and high-resolution details
* Allow offline usage, to reduce external server usage and energy waste.
* Power saving mode that will prioritise battery efficiency rather than app speed performance.

Serverless architecture should be recommended for more flexible scalability, where resources are pulled and ran when required rather than constantly running. Probable candidates include

* AWS Lambda
* Google Cloud functions
* Azure Cosmos DB

The addition of using Edge AI allows the processing of data locally, further reducing data transfers and power usage. Though this can only be of limited use, for if the entire app is encircled with local processing, updating and prolonged data storage will cause repercussions.

## RPA System

In General, Cloud based RPA system are generally more environmentally friendly - 7. (UiPath Inc, 2025) - provided the third party uses renewable energy. Further increasing the need to research and vet any third parties used. Cloud based servers reduce idle power consumption and remove the need for investing physical hardware, therefore also reducing electronic waste. On demand scaling is available too with cloud hosting, while on premise servers would require additional hardware to scale operations.

Security requirements may however make on-premises hosting the more viable option. If this is the case, the physical buildings should strive for the recommendations stated above. Methods can also continue to be implemented that is practiced in the cloud hosted platforms.

Redundant data should be promptly deleted or archived to lower storage space and costs. Aswell as outdated components of the RPA system that is unused.

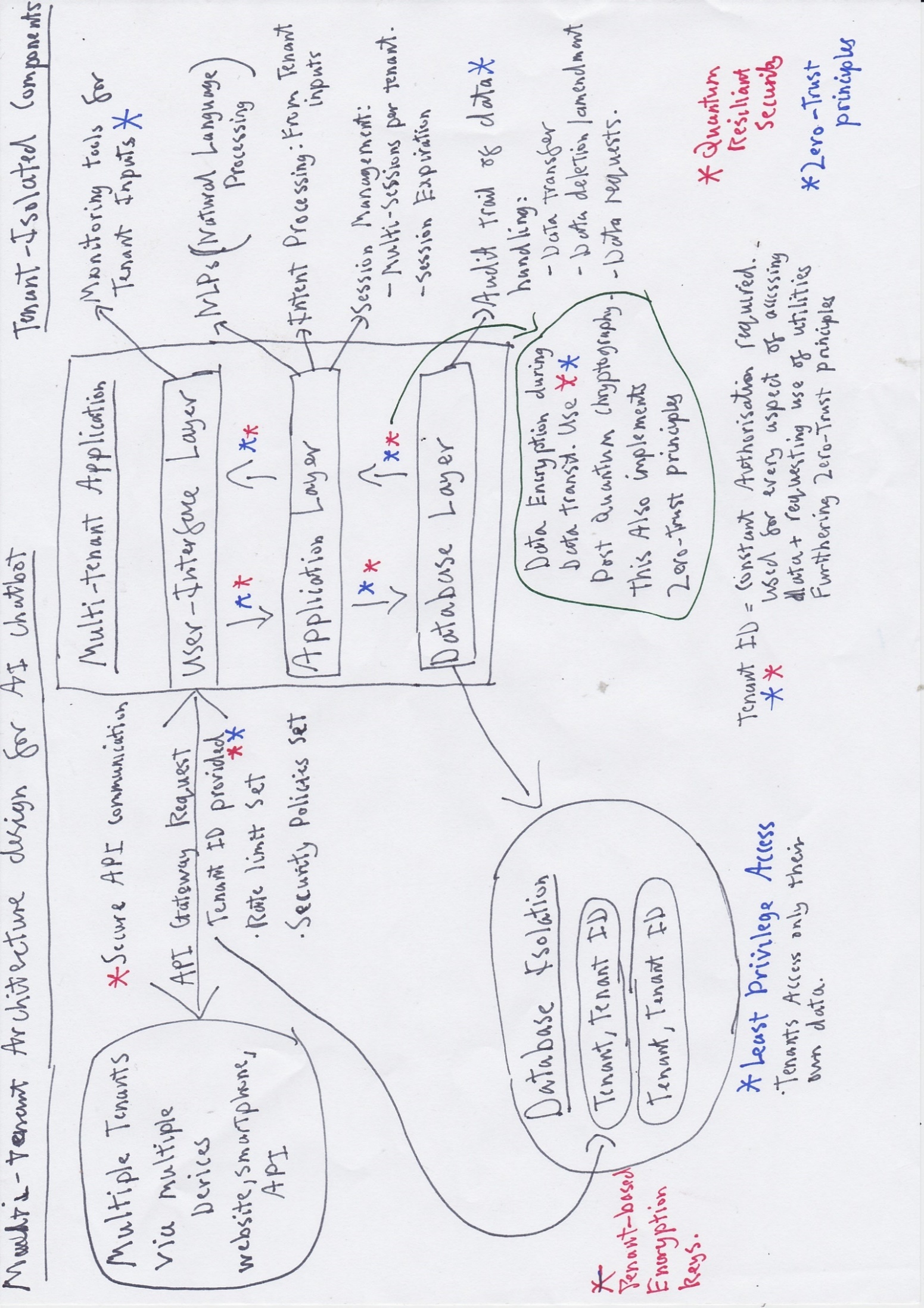
During the development lifecycle, aim for durable code to achieve fewer updates and maintenance in the future. Aswell as efficient rollout procedures for updates, decreasing data transfer sizes and frequency.

The RPA system should relieve as much physical paper – processes as possible, reducing reliance on physical documents and decreasing paper waste. Which ultimately will improve situations of deforestation and landfills, enhancing the businesses commitment to sustainable and environmentally friendly practices.

## Conclusion

Overall, renewable energy should be used when possible, or goals to replace the current power source with environmentally friendly power sources. All physical buildings and hardware should be developed or acquired with durability and recyclability in consideration. The goal is to reduce all business assets carbon footprint to as low as feasibly possible, without the interruption of operations.

# **Multi-tenant Architecture design for AI Chabot**



# **Risk Management**

## Risk Management Diagram

|  |
| --- |
|  |
| Risk Management Diagram |

## Risk Management Plan Explanation

This diagram represents a rapid and effective response plan to potential risks and incidents. With clear and precise chronological steps to ensure all aspects are addressed.

It begins with identifying what type of attack or risk that is present, along with which part of the application that is threatened / exposed. This is followed by an overall assessment of the probability this incident is / can occur, along with the feasibility of a solution. Next step is the development and integration of the decided solution. This will follow zero-trust principles 8. (NCSC, 2021) “network should be treated as compromised and therefore hostile”. All solutions and security measurements must embed quantum resilient security into them. This includes all encryption has PQC (Post Quantum Cryptography) methods.

Once the solution has been integrated to the live system, constant and detailed monitoring of how well it counters the incident must be upheld. An audit of its performance must be logged and stored until confidence for the solution is beyond a reasonable doubt. The final step will be to review all legal requirements are being met and third-party agreements have not been breached. Additionally, if necessary, the business should release a public stance of the situation, regarding the business’ accountability.

Overall, the risk plan covers with identifying and solving the incident, along with documenting and mitigating the aftermath.

## Risk Committee

It is recommended that a Risk committee is formed to govern the process. It should provide oversight and guidance for all steps and procedures. The board should represent all sectors of the business and stakeholders that are affected and involved. The committee should update the relevant higher management staff members on the plans progress and any other relevant factors. Communication between the committee members must be constant and effective, with all decisions and developments are documented.

# **References**

1. Nowsecure.com. (2023). *Post-Quantum Cryptography (PQC) & Mobile App Security - NowSecure*. [online] Available at [Post-Quantum Cryptography (PQC) & Mobile App Security - NowSecure](https://www.nowsecure.com/blog/2023/06/12/post-quantum-cryptography-pqc-mobile-app-security/) [Accessed 22 Jan. 2025].
2. Legislation.gov.uk (No date) Data Protection Act 2018. Available at: [Data Protection Act 2018](https://www.legislation.gov.uk/ukpga/2018/12/section/45) (accessed 27th January 2025)
3. Secfix.com. (2024). *ISO 27001: Protecting Businesses from Faulty AI*. [online] Available at: [ISO 27001: Protecting Businesses from Faulty AI](https://www.secfix.com/post/how-iso-27001-protects-a-business-from-wrong-working-ai#:~:text=Risk%20assessment%20and%20management%3A%20ISO,data%20breaches%2C%20or%20unauthorized%20access.) [Accessed 29 Jan. 2025].
4. Mceliece.org. (2019). *Classic McEilece: Intro*. [online] Available at: <https://classic.mceliece.org/>. [Accessed 30 Jan. 2025].
5. azure.microsoft.com. (n.d.). *Azure Sustainability—Sustainable Technologies | Microsoft Azure*. [online] Available at: <https://azure.microsoft.com/en-us/explore/global-infrastructure/sustainability>. [Accessed 30th Jan 2025]
6. UK Government (2020). *Countryside and Rights of Way Act 2000*. [online] Legislation.gov.uk. Available at: <https://www.legislation.gov.uk/ukpga/2000/37/contents>. [Accessed 30th Jan. 2025].
7. UiPath Inc (2025). *Using Cloud RPA - Future of RPA in the Cloud | UiPath*. [online] Uipath.com. Available at: <https://www.uipath.com/automation/cloud-rpa?utm_source=chatgpt.com> [Accessed 30 Jan. 2025].
8. NCSC (2021). *Introduction to Zero Trust*. [online] www.ncsc.gov.uk. Available at: <https://www.ncsc.gov.uk/collection/zero-trust-architecture/introduction-to-zero-trust> [Accessed 1st Feb, 2025]
9. National Institute of Standards and Technology (2024). The NIST Cybersecurity Framework (CSF) 2.0. *The NIST Cybersecurity Framework (CSF) 2.0*, [online] 2.0(29). doi:https://doi.org/10.6028/nist.cswp.29. [Accessed 6th Feb, 2025]