**STRUCTURED APPLICATION**

Contents

[**MOBILE BANKING APP** 1](#_Toc189098497)

[Diagrams of Scrum and Agile methodology 1](#_Toc189098498)

[Justification for Scrum – Agile hybrid methodology (289) 1](#_Toc189098499)

[Security for the Mobile App 1](#_Toc189098500)

[Quantum Resilient Security 1](#_Toc189098501)

[Supply Chain 1](#_Toc189098502)

[**AI POWERED CHATBOT** 1](#_Toc189098503)

[Diagrams of CRISP-DM and HCAI methodology 1](#_Toc189098504)

[Justification for CRISP-DM and HCAI hybrid methodology 1](#_Toc189098505)

[Security for the AI chatbot 1](#_Toc189098506)

[Supply Chain Security 1](#_Toc189098507)

[**RPA (ROBOTIC PROCESS AUTOMATION) SYSTEM** 1](#_Toc189098508)

[Diagrams of DevSecOps – Lean Six Sigma methodology 1](#_Toc189098509)

[Justification for DevSecOps and Lean Six Sigma hybrid methodology 1](#_Toc189098510)

[**References** 1](#_Toc189098511)

# **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* |

|  |
| --- |
|  |
| 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 (289)

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.

## Security for the Mobile App

### Quantum Resilient Security

For the Area of the Mobile App, QRS applications are essential for securing the abundance of sensitive data. This will focus on integration encryption methods into the mobile to withstand attacks by quantum apparatus to ensure the safe transfer and storage of data. It is recommended to use the guidelines set out by the National Institute of Standards and Technology (NIST) for future guidance.

#### Part 1: Securing the access of the app/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.

#### Part 2: Data Transfer/Storage

* 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.

### Supply Chain

Dependency management must be maintained expertly to mitigate risk. A zero-trust approach should be used for all third-party components. Third party sectors can include infrastructure/ cloud storage, data analytics, customer support and communications and authentication

Checking the third parties source code should be a standard requirement. Verify by:

* Researching if the third-party software is open/closed source,
* Thorough documentation of all changes and updates have been kept,
* Running tools such as Static and Dynamic code analysis to identify potential vulnerabilities or program errors.

Using third party components will greatly optimize cost and functionality, however thorough analysis will be required before implementation takes place. Third parties that are popular and have a strong reputation of reliability should be recommended (such as Mastercard, Visa, SendGrid, Microsoft Azure).

# **AI POWERED CHATBOT**

## Diagrams of CRISP-DM and HCAI methodology

|  |
| --- |
|  |
| CRISP-DM & HCAI Diagram A |

|  |
| --- |
|  |
| CRISP-DM & HCAI Diagram B.1 |

|  |
| --- |
|  |
| CRISP-DM & HCAI Diagram B.2 |

|  |
| --- |
|  |
| CRISP-DM & HCAI Diagram B.3 |

## 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

## Security for the 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 (ROBOTIC PROCESS AUTOMATION) SYSTEM**

## Diagrams of DevSecOps – Lean Six Sigma methodology

|  |
| --- |
|  |
| *Entire DevSecOps – Lean Six Sigma Methodology Diagram A* |

|  |
| --- |
|  |
| *Entire DevSecOps – Lean Six Sigma Methodology Diagram B.1* |

|  |
| --- |
|  |
| *Entire DevSecOps – Lean Six Sigma Methodology Diagram B.2* |

|  |
| --- |
|  |
| *Entire DevSecOps – Lean Six Sigma Methodology Diagram B.3* |

|  |
| --- |
|  |
| *Entire DevSecOps – Lean Six Sigma Methodology Diagram B.4* |

|  |
| --- |
|  |
| *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 for the 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.

# **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 McEliece: Intro*. [online] Available at: <https://classic.mceliece.org/>. [Accessed 30 Jan. 2025].