1. Scope Public Statement

The scope of XY Innovates Information Security Management System (ISMS) covers the organization's digital wallet services and related software development activities at the Newcastle office. It includes protecting critical customer data, digital wallet software, financial records, accounting information, and human resources data. The ISMS aims to ensure compliance with relevant financial and industry regulations, mitigate security risks, and restore customer confidence following recent organizational changes and cyberattacks. The focus is on strengthening essential services through robust security measures to achieve ISO 27001 certification.

In addition to this the isms scope would take into consideration the Statement of applicability which presents all the controls that would need to implement or developed to meet the iso27001 requirements and to be able to address al of the issues and concerns that xy innovate may not be privy to. The aim of this in to strengthen xy innovates services and organisation by impending security measures.

2. Scope Boundaries

Organisational boundaries

The ISMS scope for the organisational boundaries would include the individuals and departments that are involved in securing and managing the digital wallet application which ensures that the correct individuals are able to focus their attention to proving the best possible services.

<u>Digital wallet services Team-</u>

- Executive vice president – The individuals responsible for this is Jamie lee and he provides an oversight of the digital wallet service
- Digital Wallet Software Services Manager- The person responsible for this would be Nisha Kaur and this individual oversees the software and technical aspect of this service
- Manager of Software Development – The Individual responsible for this would be Mike Rogers and he leads the software development for the digital wallet.
- Supervisor Information Security – The individual responsible for this would be Chloe Davis. This individual is responsible for monitoring and managing the ISMS related security controls
- Wallet App Designer – The individual responsible for this would be Micheal Brown. He would design and develop security for users to use our services in a safe way.
- Lead Programmers- The individuals responsible for this would be a joint effort from Olivia and Ethan. These 2 would implement and maintain the digital wallets coding database and backend servers.

IT Team

- IT Supervisor – the individual responsible for this rile is Peter Knowles and his job is to ensure that the IT infrasture is safe and secure for the digital wallet use
- Network Technician – The individuals that are responsible for this would be Ethan and Jacob with their specific job being to maintain the network infrastructure for the organization to ensure secure connectivity.
- Support Technicians – the individual responsible for dealing with this would be Ethan and riley these 2 individuals would provide technical support for ISMS related it tasks.

Administration Team

Finance manager – the individual in this position is Micheal Wilson with the responsibility to maintain and oversee the financial data security with regards to the relevant pci dss and financial regulations.

Legal and Compliance officer – The person in this position is Benjamin Harris and the responsibility of this individual is to ensure that the ISMS is compliant with the correct legal and regulatory frameworks

HR Manager – The individual responsible for this position would be Sarah Harris and the responsibility is to maintain and mange sensitive HR data of the organisation.

Information system boundaries -

The boundaries of the ISMS scope include three essential areas: organizational, information system, and physical boundaries. All vital assets within these areas—such as the digital wallet software, customer financial information, security systems, and associated documentation—are protected by the ISMS. This approach guarantees thorough security for XY Innovates primary digital wallet services operating in the London and Newcastle offices.

Other key boundaries include –

1) Windows 11 operating system which is utilised across the organization by the employees
2) Internal network Infrastructure – this ensures that we are facilitating secure communications across the organisation
3) VPN solutions are used to ensure a level of security for remote access when accessing sensitive applications and data.

Physical Boundaries -

The physical boundaries of the ISMS encompass the two primary offices: the London office and the Newcastle office

At the Newcastle office, a network connects to a central server responsible for storing customer data, financial information, and transaction records. A dedicated file server also maintains critical information, including transaction records, customer details, financial records, partnership agreements, and compliance documentation.

To ensure the security and integrity of systems within these boundaries, XY Innovate employs two key features: one central server that manages transactions and payment applications, and a second system that safeguards sensitive information such as customer data and compliance documents.

The physical boundaries of the ISMS encompass the two primary offices: the London office and the Newcastle office

1) The Newcastle office is where the software development teams re situation which have the direct focus on maintaining the digital wallet application
2) London Head Office is where xy innovate house their administrative functions and the key individuals associate with the organisation

Key assets to be protected inside the scope -

- Digital Wallet Software (Design and architecture of the digital wallet software, Source code and other technical elements, Development costs and strategic planning documents)
- Customer and Partner Information (Customer database, including personally identifiable information (PII) and payment information, Contracts with payment gateways, banks, and identity verification services, Partnership agreements and employee contracts)
- Financial and Accounting Data (Financial records, transaction logs, accounting information, Data related to revenue streams from digital wallet services)
- Human Resources Information (Employee records, including roles and responsibilities, Payroll and other sensitive employee data)

3. Research and Justification of What Assets are Included and Excluded from the Scope

3.1 Included assets

The critical assets within XY Innovates ISMS scope focus on securing digital wallet services and protecting customer data.

<u>Digital wallet</u> - This includes its architecture, design, and source code—which safeguards financial transactions. Additionally, customer financial data, including transaction records and personally identifiable information (PII), is a key focus, requiring strict compliance with regulations to maintain customer trust and data integrity.

The Justification behind this is that according to the ISO/IEC 27001:2022 framework the process of ensuring integrity and confidentiality of the digital wallet application is directly linked to the overall security of the infrastructure and they have a direct correlation to overall security. Additionally academic research conducted by Dhillon (2019) highlights the significance of ensuing robust and efficient software security is an important factor to reduce and prevent cyberattacks and to ensure a level of smoothness when operating with financial transactions within the digital wallet application.

<u>Customer Financial data </u>– This asset includes personally identifiable information (PII) which would arise from the customers financial information when they would use our application to conduct online financial transactions in their day to day lives. This process is extremely important to supporting secure financial assets and ensuring they are meeting the regulatory requirements such as GDPR.

By protecting customers financial data, we ensure that the data can not be exposed to vulnerabilities which would in return enforce that sense of customer trust. As we can see from the literature by Von Solms and Van Niekerk, providing a layer of security and safeguarding PII forms the foundation of organization security. The research also shows that well managed data security strengthens the customers trust in our ability as an organisation.

3.2 Excluded Assets

Assets excluded from the ISMS scope are those that do not directly impact the digital wallet service at XY Innovate's Newcastle office. For example, **office printers and scanners** are used solely for routine administrative tasks and have no significant role in safeguarding or maintaining the business's core systems, such as financial data management. By excluding these, the ISMS can focus its security efforts on enhancing and protecting the digital wallet service, while still adhering to comprehensive organizational security policies for overall protection.

4. Research and Justification Regarding the Size of Scope

I have chosen the size of this scope to be set as a limited this is because xy innovative only focus on the most critical components related to the security and maintenance of the digital wallet service.

This focus on a few key critical components allows much more control over essential systems while allocating the correct number of resources required

- Digital wallet software- this covers the designs, the source code, technical architecture which is essential to secure financial transaction
- Customer financial information- this focuses on customer database which stores personally identifiable information (PII)
- cloud infrastructure - this encapsulated the digital ocean's data storage system that we have utilised.

Justifications as to why the scope is Limited-

1. resource efficiency - the organisation has much more control over the allocation of resources to manage assets such as customer data , infrastructure and servers. This aligns with Nist SP 800-53 security framework as this emphasizes the importance of resource allocation based on risk assessment.(NIST,2020)
2. Regulatory compliance focus - due to smaller scope size the company is able to focus on compliance with industry regulations ensuring that key processes and services are secured. This is highlights in clause 4 of the /IEC 27001:2013 as this allows the organization to understand the context by addressing the necessary regulatory requirements.(ISO/IEC 27001:2013)
3. Enhanced control and monitoring - the isms can maintain a increased level of control over the key critical infrastructure and systems which leads to more focus and being able to identify new threats to protect against cyber attacks. As highlighted in Gartner Research (2021) when you implement a structured isms this improves an organisation's ability o monitor and mange security risks which leads to increased and improved security.

National Institute of Standards and Technology (NIST), 2020. *NIST Special Publication 800-53 Revision 5: Security and Privacy Controls for Information Systems and Organizations*. [pdf] Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf [Accessed 1 November 2024].

ISO/IEC. (2013). *ISO/IEC 27001:2013*

Information Technology – Security Techniques – Information Security Management Systems – Requirements. International Organization for Standardization, Section 4

Gartner, 2024. *Information Security Strategy*. [online] Available at: https://www.gartner.com/en/cybersecurity/topics/information-security-strategy [Accessed 1 November 2024].

Dhillon, G. (2019). *Information Security Management: Concepts and Practice*. 1st ed. Springer. Available at : Unraveling Complexity in Information Systems Security Management (Accessed: 6 January 2024).

ISO/IEC 27001:2022. *Information Security, Cybersecurity, and Privacy Protection — Information Security Management Systems — Requirements*. International Organization for Standardization. Available at: ISO/IEC 27001:2022 - Information security management systems (Accessed: 6 January 2024).

Von Solms, R. and Van Niekerk, J. (2013). 'From information security to cyber security', *Computers & Security*, 38, pp. 97–102. Available at: From information security to cyber security | Computers and Security (Accessed: 6 January 2024).