Introduction

Continued technological advancements and change in consumer behaviours is making online shopping systems a strategic imperative for businesses across industry. In Europe the percentage of the population purchasing goods or services online nearly doubled from 30 percent in 2007 to 57 percent by 2017. The same trend can be seen in online grocery shopping. Take the UK for example, where online food purchases have risen from 4% in 2002 to 28% by 2017 (Statistics Netherlands, 2018).

Though the advantages for business to provide online shopping capabilities is obvious, it is important to recognise the increased cyber security and regulatory non-compliance risks this brings. In 2021, the average cost of a cyber-attack for small businesses ranged from $120,000 to $1.24 million (Sharif & Mohammed, 2022). Wolford B (2022) states that for a severe breach of GDPR regulation a company can be fined up to €20 million or 4% of global revenue (whichever is higher).

Targeted towards a prominent local grocery shop serving their local catchment area and expanding rapidly, the report aims to help the business understand how to implement an online shopping system that provides an efficient and secure online shopping experience for their customers.

User Requirements

This report leverages the Unified Modelling Language (UML) framework to assist with the explanation of the high-level requirements for an online shopping system. UML, a consolidation of the best practices refined over time, provides a way to present the diverse elements of a software system (e.g., requirements, data structures, data flows, and information flows) within a single framework (Seidl et al., 2015).

Top Level System Overview

Important top-level use cases to consider when implementing an online shopping system are as follows: Registration, Viewing Items, Placing Order and Checkout. Shoppers expect to save time through efficiency when grocery shopping online (Anesbury et al., 2016). A simple, intuitive user experience should be foundational to the system design.

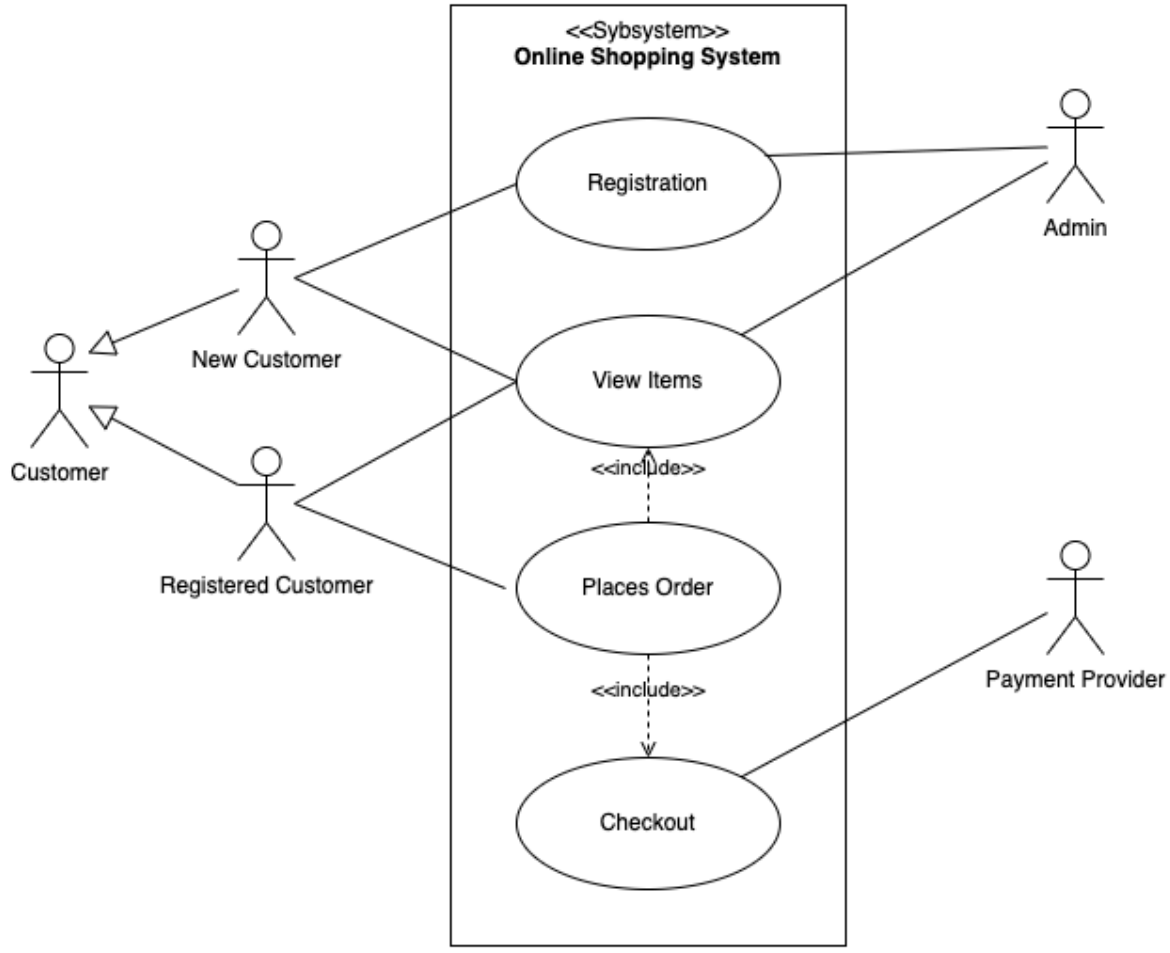

Figure 1 UML Top Level Use Case Diagram

Registration
The registration use case allows for a customer or employee user to create accounts, log in to the system, and manage their profile details.

View Items

Viewing items should include several optional use cases: search items, Browse product, View recommended items, Add to favourites, Add to shopping cart. Searching should be robust, with filter capability and categorisations. A study by Anesbury et al., (2016) states that shoppers expect to see their favourite brands quickly, and easy-to-use search options that make it easy for shoppers to discern where their preferred brand(s) are is important. The system should ensure customer authentication is included to ensure personalisation.

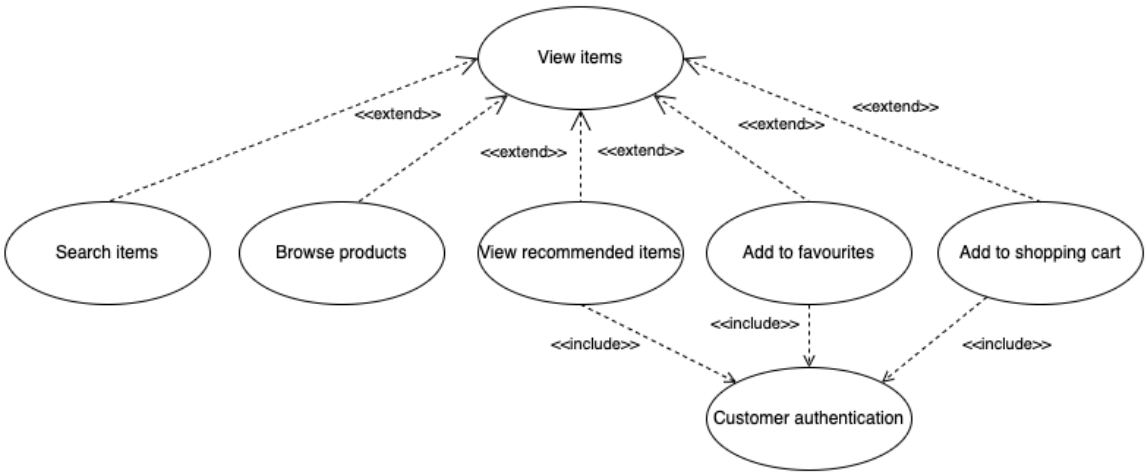

Figure 2 UML View Items Diagram

Place Order and Checkout

Figure 3 provides a visual representation of the proposed process flow. Payment options should offer flexibility such as use of either a credit / debit card or PayPal. Customer authentication should once again be included for personalisation. Payment options should offer flexibility, with the use of either a credit or debit card and PayPal.

As the online shopping system will handle payments, it is proposed that the system is compliant with or certified to Payment Card Industry Data Security Standard (PCI DSS). PCI DSS is an important part of compliance for businesses that accept credit card (Anderson, 2020). This involves implementing basic hygiene for any systems holding cardholder data such as account numbers and expiry dates while sensitive data such as CVVs and PINs can’t be stored at all.

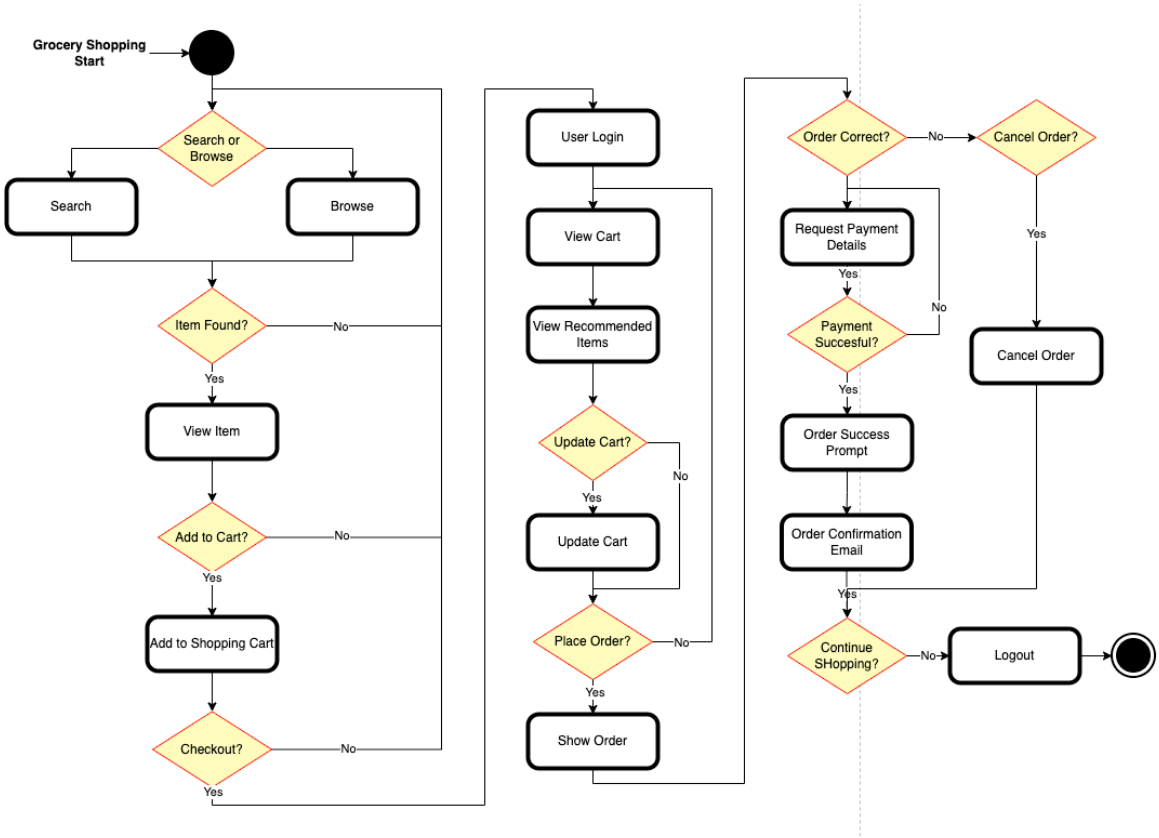

Figure 3 UML Activity Diagram

Cyber Security & Privacy Considerations

The main aspect of the software design process, from a security viewpoint, is threat modelling as it enables a better understanding of the system and helps identify system defects early on (LeBlanc & Howard, 2002).

The following three step methodology was followed to determine potential cyber threats relevant to an online shopping system.

1. **Decomposed The System**

Having a data flow diagram (DFD) is important to determine threat targets such as data sources, process, data flows, interactors, and actors (LeBlanc & Howard, 2002).

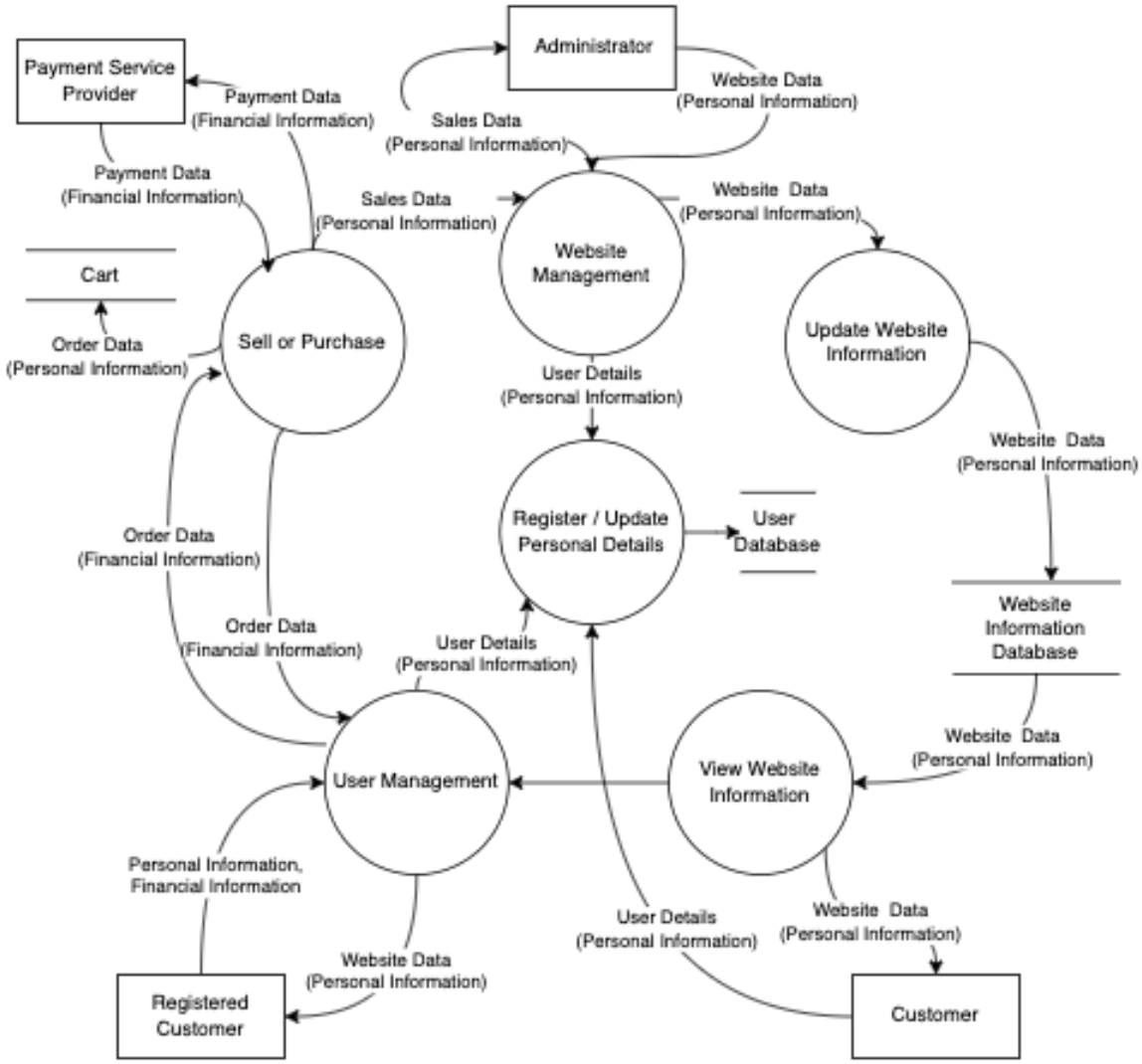

Figure 4 DFD Diagram of Online Shopping System (OSS)

2. Identify Potential Threats with STRIDE

Developed by Microsoft employees, STRIDE is an acronym that represent six key threat categories (LeBlanc & Howard, 2002):

Spoofing identity: Unauthorized entities such as an actor or server pretending to be someone else.
Tampering with data: Malicious modification of data.
Repudiation: Users who deny performing an action.
Information disclosure: Exposure of information to individuals who should not have access to it.
Denial of service (DoS): DoS attacks disrupt service to authorised users.
Elevation of privilege: Unprivileged user gains privileged access, allowing them to compromise or damage the system.

STRIDE was used to begin building out potential threats for further analysis.

3. Build Threat Trees

Threat trees describe the decision-making process a potential attacker could go through to compromise the online shopping system (LeBlanc & Howard, 2002). Once high threats had been determined using STRIDE, threat trees were used to analyse them further.

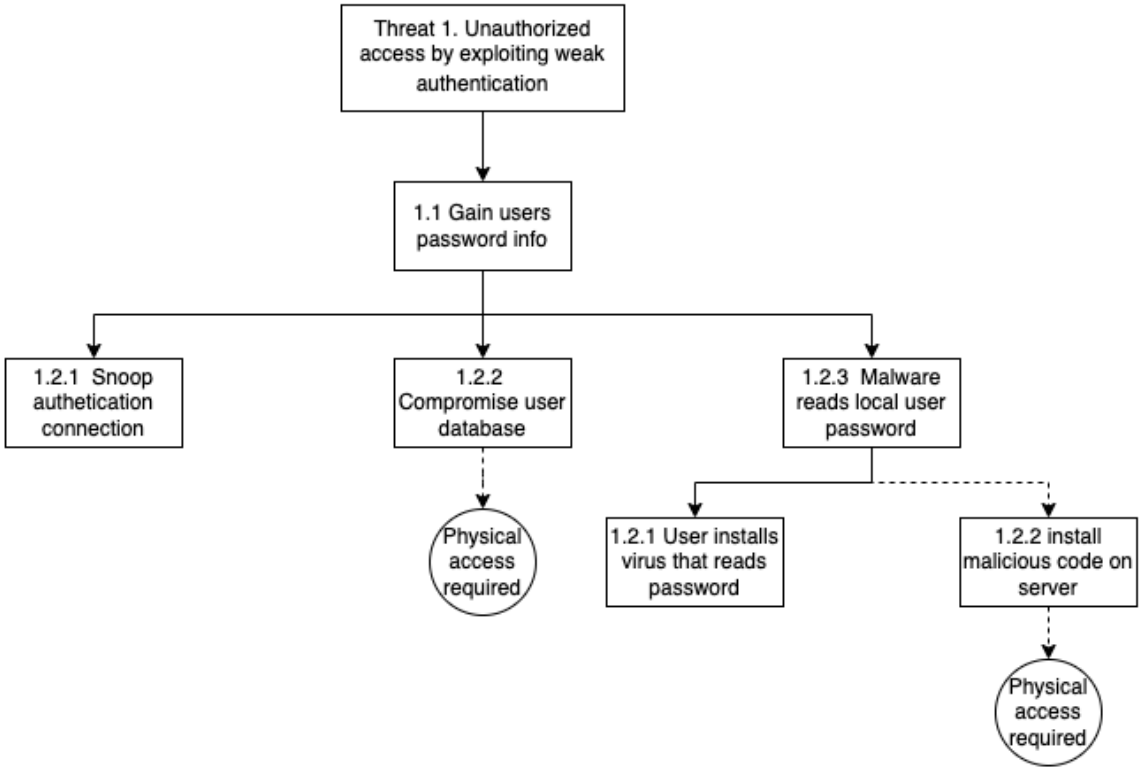

Figure 5 Example Threat Tree Mapping

Assessment Results

Table 1 provides the threat assessment results.

Table 1 Threat Assessment Results

ID	Threat	STRIDE	Proposed Control
1	Unauthorized access by exploiting weak authentication	S	Regular Security Audits Penetration Testing Access Controls Firewalls Secure Coding Practices Security Training and Awareness Incident Response

2	Deploy rogue web pages or code	T	Regular Security Audits Penetration Testing Penetration Testing Data Encryption at Rest Firewalls Vulnerability Management Secure Coding Practices Security Training and Awareness Incident Response Vendor Security Assessments
3	Manipulation of product prices or customer information		
4	Denying responsibility for transactions	R	Regular Security Audits Penetration Testing Incident Response
5	Unauthorized access to sensitive customer or business data	I	Regular Security Audits Penetration Testing Data Encryption in transit Incident Response
6	Overwhelming the online store's capacity to disrupt services	D	Regular Security Audits Penetration Testing Incident Response
7	Gaining unauthorized access to administrative functions by leveraging the service client request process.	E	Multi-Factor Authentication (MFA) Regular Security Audits Penetration Testing Access Controls Vulnerability Management Incident Response Vendor Security Assessments

Proposed Control Details

Proposed control details for addressing the identified threats, including rationale for inclusion and implementation guidance can be found in table.

Table 2 Proposed controls to address identified threats.

Proposed Control	**Rationale for Inclusion**	**Implementation Guidance**
Multi-Factor Authentication (MFA)	MFA requires two or more independent authentication factors, ensuring a more rigorous authentication process. Even if one factor is compromised, the likelihood	Implement MFA for both Customer and Employee authentication

	of a successful breach is still reduced (Fanti, 2023).	
Penetration Testing	A penetration tests are simulated attacks against systems that mimics a real-life attack to identify and validate vulnerabilities, configuration issues, and business logic flaws (Viegas et al., 2022).	Perform regular penetration testing to help ensure your cyber security posture remains relevant to a changing threat landscape over time.
Data Encryption in transit	SSL/TLS supports bi-directional encryption and authentication, ensuring that data transmitted between the customer's web browser and the online store's server is encrypted, helping protect data transfer from eavesdropping and manipulation (Anderson, 2020).	Firstly, identify and maintain an understanding of the flow of data from its origin to its final destinations to ensure all paths are known (LeBlanc & Howard, 2002). Next, secure these paths by using encryption protocols like TLS or HTTPS to secure data transmission between them.
Data Encryption at Rest	When storing sensitive data, encrypt the data rather than store it in plaintext by using a good cryptographic algorithm and well-protected key. Encrypting stored data protects against unauthorized access. (LeBlanc & Howard, 2002).	Encrypt all data at rest.
Access Controls	Anderson (2020) states the main function of access control is to mitigate the harm that can be done by groups, users, and programs whether through error or malice.	Assess relevant vendors cyber security posture for appropriate security practices helps mitigate risks associated with outside organisations. Assess any third-party vendors performing any data-related functions like payment processing.
Firewalls	Firewalls and IPS help prevent the risk of unauthorised access by an outsider from an outside network that can lead to threats including network access attacks, Denial of Service (DOS) attacks, and reconnaissance attacks. (Anderson, 2020).	Use firewalls and IPS to prevent unauthorised access to the company network and its services from other external networks.
Secure Coding Practices	Code review involves reviewing the source code of an application or	Implement secure coding practices like threat modelling,

	system by a competent reviewer with the goal of detecting logic errors, vulnerabilities, potential defects (Viegas et al., 2022).	code reviews and testing into the SDLC to reduce the likelihood of vulnerabilities.
Security Training and Awareness	Frequent security training is required because the security landscape changes rapidly as new threats are found (LeBlanc & Howard, 2002).	Train employees on the importance of data security, privacy, and compliance.
Incident Response	An incident response plan is required to respond to a newly discovered vulnerability or an attack (Anderson, 2020).	Implement a robust incident respond capability for handling information security and privacy events including potential data breaches. The process should ensure notification of any interested party as required by law.
Vendor Security Assessments	LeBlanc & Howard (2002) argues that if your company works with untrustworthy partners, people will view your company as untrustworthy.	Assess relevant vendors cyber security posture for appropriate security practices helps mitigate risks associated with outside organisations. Assess any third-party vendors performing any data-related functions like payment processing.

Data Privacy Considerations

Respecting customer privacy is crucial to building trust. People will not feel comfortable purchasing your products and services unless they trust you. (LeBlanc & Howard, 2002).

Addressing the following data privacy areas over and above implementing the proposed cyber security controls will create a secure and trustworthy online shopping system for customers while helping ensure compliance with data protection laws and regulations. The requirements are based on the European Union's General Data Protection Regulation (GDPR).

GDPR Data Protection Principles (Wolford, 2022)	Requirement Information (Wolford, 2022)	Proposed Approach
Lawfulness, fairness, and transparency	Processing must be legal and just, and transparent to the data subject.	Clearly communicate about what data you plan to collect, how it will be used, and who it may be shared with. Maintain a transparent privacy policy

		that is accessible to everyone. For each continual release, the policy should be reviewed again (LeBlanc & Howard, 2002).
Purpose limitation	You must process data for valid purposes clearly communicated to the data subject when you collected it	Establish a data retention policy that includes data retention and deletion (deleted once it is no longer needed for business purposes or legal compliance) requirements.
Storage limitation	You may only store personally identifying data for as long as necessary for the specified purpose.	
Data minimization	You should collect and process only the minimum essential data necessary for the purposes specified.	Only collect the minimum customer data required. When users have access to sensitive information, they will be tempted to view it so ensure audit logging is enabled (LeBlanc & Howard, 2002).
Accuracy	You must keep personal data accurate and current.	Implement procedures for regular evaluation of the accuracy of customer and employee data.
Integrity and confidentiality	Processing must be done securely to ensure appropriate security, integrity, and confidentiality of data.	When storing sensitive data, encrypt the data rather than store it in plaintext by using a good cryptographic algorithm and well-protected key. Encrypting stored data protects against unauthorized access. (LeBlanc & Howard, 2002).
Accountability	The data controller must be able to demonstrate GDPR compliance with all these principles.	Perform regular privacy audits that seek out evidence to conformance.

Conclusion

In summary, this report provides guidance to help a grocery business understand how to implement an online shopping system. Research confirms both the advantages for business to provide online shopping capabilities and recognises the increased cyber security and regulatory non-compliance risks this brings. In conclusion if a business ensures the system design provides an intuitive and timely user experience and invests appropriately in the required cyber security and data privacy controls, they can implement an efficient and secure online shopping experience for their customers.

References:

Anderson, T. (2020) *Security Engineering: A guide to building dependable distributed systems.* 3rd ed. Indianapolis, Indiana: John Wiley & Sons, Inc.

Anesbury, Zachary et al. (2016) *How Do Shoppers Behave Online? An Observational Study of Online Grocery Shopping.* Journal of consumer behaviour 15.3 (2016): 261–270.

Fanti, Marco. (2023) *Implementing Multifactor Authentication: Protect Your Applications from Cyberattacks with the Help of MFA.* 1st ed. Birmingham, England: Packt Publishing Ltd.

LeBlanc, David, and Michael Howard. (2002) *Writing Secure Code.* United States: Pearson Education, Limited.

Seidl, Martina, et al. (2015) *UML @ Classroom: An Introduction to Object-Oriented Modeling,* Springer International Publishing AG,. ProQuest Ebook Central. Available from: http://ebookcentral.proquest.com/lib/universityofessex-ebooks/detail.action?docID=6314177 [Accessed 7 January 2024].

Statistics Netherlands (2018) Netherlands in EU top 5 online shopping, September 19. Downloadable via https://www.cbs.nl/en-gb/news/2018/38/netherlands-in-eu- top-5-online-shopping.

Sharif MH, Mohammed MA. (2022) *A literature review of financial losses statistics for cyber security and future trend.* World Journal of Advanced Research and Reviews 2022, 15(01): 138–156.

Viegas, Virgilio, and Oben Kuyucu. (2022) *IT Security Controls: A Guide to Corporate Standards and Frameworks.* Place of publication not identified: Apress.

Wolford, B. (2020) *What is GDPR, the EU's new data protection law?* Available from: https://gdpr.eu/what-is-gdpr/ [Accessed 08 November 2023].