System Security Plan

E-Commerce System

Version 1.0

Approved By: _____ Approval Date: _____
Insert Approver Title

Approved By: _____ Approval Date: _____
Insert Approver Title

Approved By: _____ Approval Date: _____
Insert Approver Title

Table of Contents

E-Commerce Submodule Legend

User Management and Authentication	Blue
Product Catalog and Inventory Management	Gray
Order Processing and Fulfillment	Orange
Shopping Cart and Checkout	Violet
Payment Gateway Integration	Gold
Customer Reviews and Ratings	Green
Recommendation Engine	Pink
Reporting and Analytics	Brown

1 Document Revision History

Version	Date	Author	Description
1.0	11/28/2023	BSIT 3-1	First version of the System Security Plan for BSIT 3-1 (S.Y. 23 – 24) E-Commerce System.

2 Executive Summary

The primary goal of the E-Commerce System is to establish a comprehensive and user-friendly website catering to both customer and employee administration needs. Compromising key submodules such as User Management and Authentication, Product Catalog and Inventory Management, Order Processing and Fulfillment, Shopping Cart and Checkout, Payment Gateway Integration, Customer Reviews and Ratings, Recommendation Engine, and Reporting and Analytics. With the submodules mentioned, the system will be able to offer features that will ensure efficiency, security, and ease to its users.

With a focus on secure user authentication and management, dynamic product inventory control, and streamlined order processing, the system optimizes the end-to-end customer journey. In addition, a user-friendly shopping cart, secure payment gateway, customer review and ratings, and a recommendation engine for products enhances the overall customer experience. Furthermore, the reporting and analytics provide valuable insights for informed decision making.

The developers of each submodule included in the E-Commerce System are responsible for ensuring the functionality and integration of their respective components. For instance, the User Management and Authentication developers focus on creating a secure authentication system while prioritizing the security of user data. While Product Catalog and Inventory Management developers are responsible for organizing and displaying the products in a visually appealing manner, as well as controlling its inventory. As for the Order Processing and Fulfillment, the developers are expected to optimize the entire order cycle, from order placement to delivery. Moreover, the Shopping Cart and Checkout developers are assigned to create a user-friendly interface with features to enhance customer buying experience. Afterwards, the Payment Gateway Integration developers are dedicated to making sure that secure and smooth financial transactions are met. Additionally, the Customer Review and Ratings developers aim to collect customer feedback and engagement by allowing them to share their insights and experiences. In addition to that, the Recommendation Engine developers hold the responsibility to provide personalized product suggestions to customers based on their preferences. Lastly, the Reporting and Analytics developers focus on providing informative insights on the overall performance and evaluation of the E-Commerce System.

In essence, a collaborative effort from the submodule's respective teams ensures that each of the system's submodules will be able to meet its standards in a timely manner. Utilizing this collaborative approach will enable the developers of the E-Commerce System to achieve their objectives. This synchronization will effectively enhance the efficiency and functionality of each submodule and integrated user experience.

3 System Identification

System Name: E-Commerce System
System Type: E-Commerce

System Submodules: User Management and Authentication, Product Catalog and Inventory Management, Order Processing and Fulfillment, Shopping Cart and Checkout, Payment Gateway Integration, Customer Reviews and Ratings, Recommendation Engine, and Reporting and Analytics.

Information System Owner	
Name	Rosicar E. Escober
Title	PhD
Department	
Phone Number	
Email	

Information System Management	
Name	Shane Steven Servas
Title	Project Manager of Submodule I
Department	User Management and Authentication
Phone Number	09154269979
Email	shanestevenservas.acad@gmail.com

Information System Management	
Name	John Paulo Battung
Title	Project Manager of Submodule II
Department	Product Catalog and Inventory Management
Phone Number	09613106491
Email	battungpaulo@gmail.com

Information System Management	
Name	Daniel Del Rosario
Title	Project Manager of Submodule III
Department	Order Processing and Fulfillment
Phone Number	09565583168
Email	danidel12360@gmail.com

Information System Management	
Name	Rozzelle De Omania
Title	Project Manager of Submodule IV
Department	Shopping Cart and Checkout
Phone Number	09468723835
Email	rozzelledeomania0330@gmail.com

Information System Management	
Name	Kirsten Charles Domingo
Title	Project Manager of Submodule V
Department	Payment Gateway and Integration
Phone Number	09254916837
Email	kcdomingo25@gmail.com

Information System Management	
Name	Jarrell Reyes
Title	Project Manager of Submodule VI
Department	Customer Review and Ratings
Phone Number	09564330929
Email	jrrllrey17@gmail.com

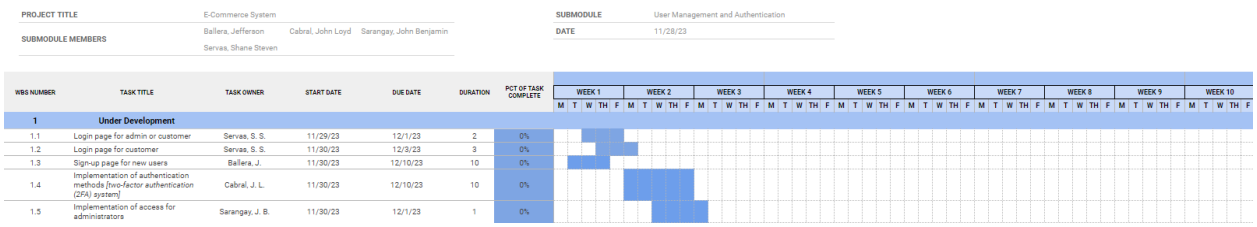
Information System Management	
Name	Kimberly Mae Kho
Title	Project Manager of Submodule VII
Department	Recommendation Engine
Phone Number	09205119555
Email	kimlykho27@gmail.com

Information System Management	
Name	Joshua Chua
Title	Project Manager of Submodule VIII
Department	Reporting and Analytics
Phone Number	09066001123
Email	joshuaannatuchua20@gmail.com

4 System Operational Status

1. User Management and Authentication (Under Development)

- Login page for admin or customer
- Login page for customer
- Sign-up page for new users
- Implementation of authentication methods *[two-factor authentication (2FA) system]*
- Implementation of access for administrators



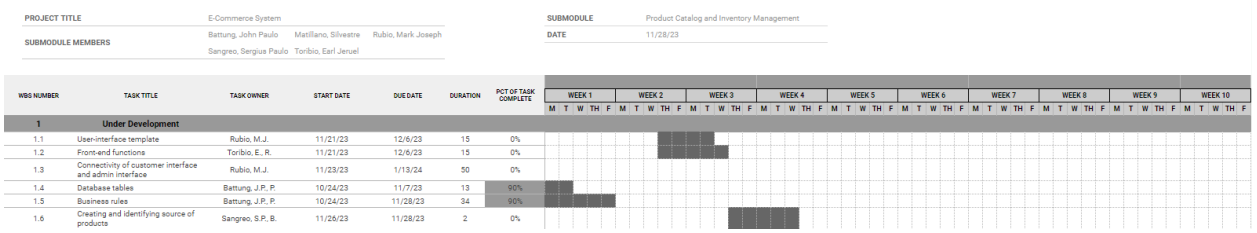
PROJECT TITLE: E-Commerce System
SUBMODULE MEMBERS: Ballera, Jefferson; Cabral, John Loyd; Sarangay, John Benjamin; Servas, Shane Steven
SUBMODULE: User Management and Authentication
DATE: 11/28/23

WBS NUMBER	TASK TITLE	TASK OWNER	START DATE	DUE DATE	DURATION	PCT OF TASK COMPLETE
1	Under Development					
1.1	Login page for admin or customer	Servas, S. S.	11/29/23	12/1/23	2	0%
1.2	Login page for customer	Servas, S. S.	11/30/23	12/3/23	3	0%
1.3	Sign-up page for new users	Ballera, J.	11/30/23	12/10/23	10	0%
1.4	Implementation of authentication methods *[two-factor authentication (2FA) system]*	Cabral, J. L.	11/30/23	12/10/23	10	0%
1.5	Implementation of access for administrators	Sarangay, J. B.	11/30/23	12/1/23	1	0%

WEEK 1 | WEEK 2 | WEEK 3 | WEEK 4 | WEEK 5 | WEEK 6 | WEEK 7 | WEEK 8 | WEEK 9 | WEEK 10
M T W TH F M T W TH F M T W TH F M T W TH F M T W TH F M T W TH F M T W TH F M T W TH F M T W TH F M T W TH F

2. Product Catalog and Inventory Management (Under Development)

- User-interface template
- Front-end functions
- Connectivity of customer interface and admin interface
- Database tables
- Business rules
- Creating and identifying source of products



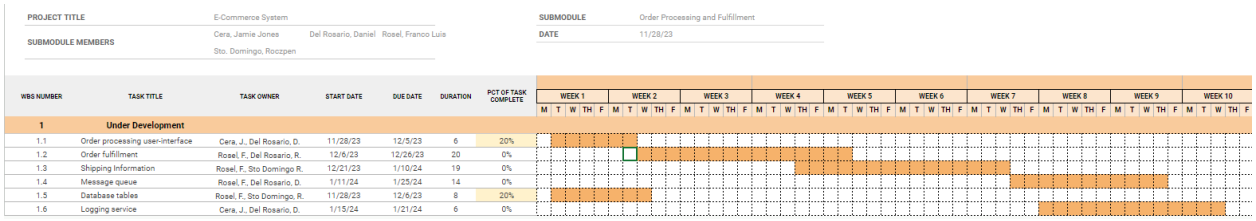
PROJECT TITLE: E-Commerce System
SUBMODULE MEMBERS: Battung, John Paulo; Matillano, Silvestre; Rubio, Mark Joseph; Sangreo, Sergius Paulo; Toribio, Earl Jeruel
SUBMODULE: Product Catalog and Inventory Management
DATE: 11/28/23

WBS NUMBER	TASK TITLE	TASK OWNER	START DATE	DUE DATE	DURATION	PCT OF TASK COMPLETE
1	Under Development					
1.1	User-interface template	Rubio, M.J.	11/21/23	12/6/23	15	0%
1.2	Front-end functions	Toribio, E., R.	11/21/23	12/6/23	15	0%
1.3	Connectivity of customer interface and admin interface	Rubio, M.J.	11/23/23	1/13/24	50	0%
1.4	Database tables	Battung, J.P., P.	10/24/23	11/7/23	13	90%
1.5	Business rules	Battung, J.P., P.	10/24/23	11/28/23	34	90%
1.6	Creating and identifying source of products	Sangreo, S.P., B.	11/26/23	11/28/23	2	0%

WEEK 1 | WEEK 2 | WEEK 3 | WEEK 4 | WEEK 5 | WEEK 6 | WEEK 7 | WEEK 8 | WEEK 9 | WEEK 10
M T W TH F M T W TH F M T W TH F M T W TH F M T W TH F M T W TH F M T W TH F M T W TH F M T W TH F M T W TH F

3. Order Processing and Fulfillment (Under Development)

- Order processing user-interface
- Order fulfillment
- Inventory service
- Message queue
- Database tables
- Logging service

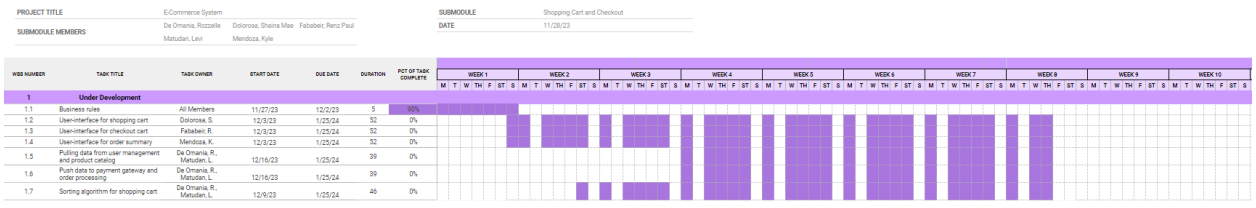


PROJECT TITLE	E-Commerce System		SUBMODULE	Order Processing and Fulfillment
SUBMODULE MEMBERS	Cera, Jamie Jones; Del Rosario, Daniel; Rosel, Franco Luis; Sto. Domingo, Roczpen		DATE	11/28/23

WBS NUMBER	TASK TITLE	TASK OWNER	START DATE	DUE DATE	DURATION	PCT OF TASK COMPLETE
1	Under Development					
1.1	Order processing user-interface	Cera, J., Del Rosario, D.	11/28/23	12/5/23	6	20%
1.2	Order fulfillment	Rosel, F., Del Rosario, R.	12/6/23	12/26/23	20	0%
1.3	Shipping Information	Rosel, F., Sto Domingo R.	12/21/23	1/10/24	19	0%
1.4	Message queue	Rosel, F., Del Rosario, D.	1/11/24	1/25/24	14	0%
1.5	Database tables	Rosel, F., Sto Domingo, R.	11/28/23	12/6/23	8	20%
1.6	Logging service	Cera, J., Del Rosario, D.	1/15/24	1/21/24	6	0%

4. Shopping Cart and Checkout (Under Development)

- Business rules
- User-interface for shopping cart
- User-interface for checkout cart
- User-interface for order summary
- Pulling data from user management and product catalog
- Push data to payment gateway and order processing
- Sorting algorithm for shopping cart

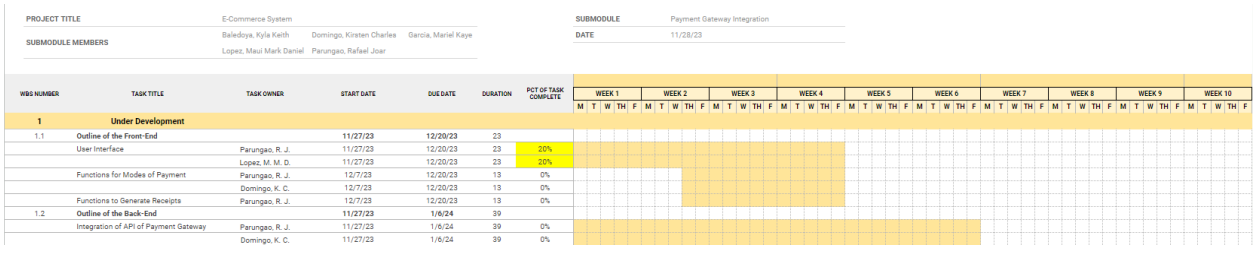


PROJECT TITLE	E-Commerce System		SUBMODULE	Shopping Cart and Checkout
SUBMODULE MEMBERS	De Omania, Rozzelle; Dolorosa, Shaina Mae; Fababeir, Renz Paul; Matudan, Levi; Mendoza, Kyle		DATE	11/28/23

WBS NUMBER	TASK TITLE	TASK OWNER	START DATE	DUE DATE	DURATION	PCT OF TASK COMPLETE
1	Under Development					
1.1	Business rules	All Members	11/27/23	12/2/23	5	50%
1.2	User-interface for shopping cart	Dolorosa, S.	12/3/23	1/25/24	52	0%
1.3	User-interface for checkout cart	Fababeir, R.	12/3/23	1/25/24	52	0%
1.4	User-interface for order summary	Mendoza, K.	12/3/23	1/25/24	52	0%
1.5	Pulling data from user management and product catalog	De Omania, R., Matudan, L.	12/16/23	1/25/24	39	0%
1.6	Push data to payment gateway and order processing	De Omania, R., Matudan, L.	12/16/23	1/25/24	39	0%
1.7	Sorting algorithm for shopping cart	De Omania, R., Matudan, L.	12/9/23	1/25/24	46	0%

5. Payment Gateway Integration (Under Development)

- Outline of user-interface
- Function or users to choose their mode of payment
- Function for users to generate their receipt
- Outline of submodule's backend development
- Integration of the API of payment gateway



PROJECT TITLE	E-Commerce System		SUBMODULE	Payment Gateway Integration
SUBMODULE MEMBERS	Baledoya, Kyla Keith; Domingo, Kirsten Charles; Garcia, Mariel Kaye; Lopez, Maui Mark Daniel; Parungao, Rafael Joar		DATE	11/28/23

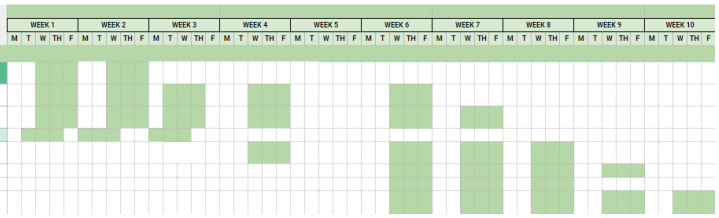
WBS NUMBER	TASK TITLE	TASK OWNER	START DATE	DUE DATE	DURATION	PCT OF TASK COMPLETE
1	Under Development					
1.1	Outline of the Front-End		11/27/23	12/20/23	23	
	User Interface	Parungao, R. J.	11/27/23	12/20/23	23	20%
		Lopez, M. M. D.	11/27/23	12/20/23	23	20%
	Functions for Modes of Payment	Parungao, R. J.	12/7/23	12/20/23	13	0%
		Domingo, K. C.	12/7/23	12/20/23	13	0%
	Functions to Generate Receipts	Parungao, R. J.	12/7/23	12/20/23	13	0%
1.2	Outline of the Back-End		11/27/23	1/6/24	39	
	Integration of API of Payment Gateway	Parungao, R. J.	11/27/23	1/6/24	39	0%
		Domingo, K. C.	11/27/23	1/6/24	39	0%

6. Customer Review and Ratings (Under Development)

- Integration with the reporting and analytics submodule
- Review and ratings user-interface under the product
- Review and ratings user-interface after buying the product
- Database tables
- Logic for requirements before commenting
- Filter for comments
- Like and dislike feature
- Filter and sorting algorithm

PROJECT TITLE	E-Commerce System			SUBMODULE	Customer Reviews and Ratings	
SUBMODULE MEMBERS	Cabacungan, Richard	Floresca, Keeperjhoi	Ko, Maverick	DATE	11/28/23	
	Padre-e, Aaron	Reyes, Jarrell				

WBS NUMBER	TASK TITLE	TASK OWNER	START DATE	DUE DATE	DURATION	PCT OF TASK COMPLETE
1	Under Development					
1.1	Integration with the reporting and analytics submodule	Padre-e, Aaron	11/29/23	12/8/23	9	70%
1.2	Review and ratings user-interface under the product	Cabacungan, Richard	11/29/23	1/7/24	38	0%
1.3	Review and ratings user-interface after buying the product	Reyes, Jarrell	11/29/23	1/14/24	45	0%
1.4	Database tables	Floresca, Keeperjhoi	11/28/23	12/17/23	19	20%
1.5	Logic for requirements before commenting	Ko, Maverick	12/20/23	1/7/24	17	0%
1.6	Filter for comments	Floresca, Keeperjhoi	1/7/31	1/14/24	7	0%
1.7	Like and dislike feature	Ko, Maverick	1/7/24	1/28/24	21	0%
1.8	Filter and sorting algorithm	Floresca, Keeperjhoi	1/7/24	1/31/24	24	0%

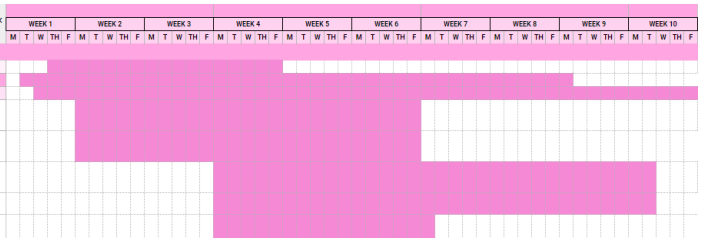


7. Recommendation Engine (Under Development)

- User-interface template
- Business rules
- Product catalog design
- Pulling data from the product catalog and inventory management submodule
- Pulling data from the order processing and fulfillment submodule
- Identification of the similar products to the user's profile of purchase history
- Identifying new and popular products
- Construction of the content-based algorithm based on user profile
- Synchronization of module's data process

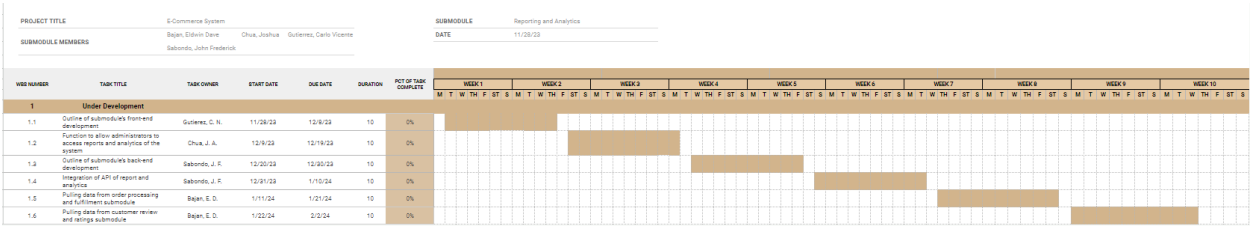
PROJECT TITLE	E-Commerce System			SUBMODULE	Recommendation Engine	
SUBMODULE MEMBERS	Kho, Kimberly Mae	Milan, Justine Mae	Orosco, Fam Ella	DATE	11/28/23	
	Pili, Erica	Torres, Julianne Dominique				

WBS NUMBER	TASK TITLE	TASK OWNER	START DATE	DUE DATE	DURATION	PERCENT OF TASK COMPLETE
1	Under Development					
1.1	User-interface template	Milan, J. M. & Orosco, F. E.	11/30/23	12/23/23	23	10%
1.2	Business rules	Kho, K. M.	11/28/23	2/2/24	64	60%
1.3	Product Catalog Design	Milan, J. M. & Orosco, F. E.	11/29/23	2/2/24	63	20%
1.4	Pulling data from the product catalog and inventory management submodule	Torres, J. D. & Pili, E.	12/4/23	1/6/24	32	0%
1.5	Pulling data from the order processing and fulfillment submodule	Torres, J. D. & Pili, E.	12/4/23	1/6/24	32	0%
1.6	Identification of the similar products to the user's profile of purchase history	Torres, J. D. & Pili, E.	12/18/23	1/31/24	43	0%
1.7	Construction of the content-based algorithm based on user profile	Torres, J. D. & Pili, E.	12/18/23	1/31/24	43	0%
1.8	Synchronization of module's data process	Torres, J. D. & Pili, E.	12/18/23	1/8/24	20	0%



8. Reporting and Analytics (Under Development)

- Outline of submodule's front-end development
- Function to allow administrators to access reports and analytics of the system
- Outline of submodule's back-end development
- Integration of API of report and analytics
- Pulling data from order processing and fulfillment submodule
- Pulling data from customer review and ratings submodule



5 General System Description

The E-Commerce System is a comprehensive and user-friendly website designed to facilitate seamless online transactions and enhance user experience. Its scope within the overall contract involves the entire e-commerce cycle from secure user authentication, product showcasing with personalized recommendations and adding items to carts, through the order processing and fulfillment, up to the completion of customers' payments, followed by the customers' review and ratings. The system serves as a centralized platform for customer interactions, inventory management, transaction processing, and generating data-driven reporting and analytics. It will ensure that the system is dedicated to supporting the business by ensuring a smooth experience for both customers and administrators.

The following major functions of the E-Commerce System include:

1. User Management and Authentication: The module manages user profiles and authentication, ensuring secure and dedicated access for customers and employee administrators. The user roles vary from guest, customer, and admin. They can choose to log in to their respective accounts, sign up to create a new account, or access the system as a guest.

2. Product Catalog and Inventory Management: The module organizes and displays products in the product catalog for customers to view, as well as managing inventory levels to provide accurate information. The administrator of the inventory management can add, view, update, archive, delete, and handle the products' description and information.

3. Order Processing and Fulfillment: The module offers listing, tracking, and updating the order placed by the customer. It showcases the process of order and its status to maintain transparency and organize orders systematically including the option to view shipment process to product delivery and history of previous purchase. The administrator has the access to control and update the order process from verification to shipment and packaging, in addition to confirming the mode of payment opted by the customer.

4. Shopping Cart and Checkout: The module provides a user-friendly shopping experience from adding, removing, viewing, managing, and searching items on their personal carts. Furthermore, allowing guests or customers to checkout items to their desired address along with their respective contact and billing information.

5. Payment Gateway Integration: The module holds responsibility for implementing a secure and reliable payment gateway within the system to facilitate smooth transactions while guaranteeing the safety and privacy of sensitive data. It includes features such as allowing customers to choose their preferred mode of payment, redirecting them to the respective payment mode page to finalize transactions. Upon completion, successful payment details are displayed to confirm the transaction's success.

6. Customer Review and Ratings: The module allows customer engagement by enabling users with the opportunity to share their insights regarding the item through reviews and ratings. This includes features where users can view the current review and ratings of an item, employ filters to search based on the number of ratings, as well expressing their preferences by liking or disliking reviews which will aid in the filtration of potentially irrelevant content. Additionally, the user can contribute their own reviews and ratings on a 1 to 5 scale for a specific item after purchase and delivery.

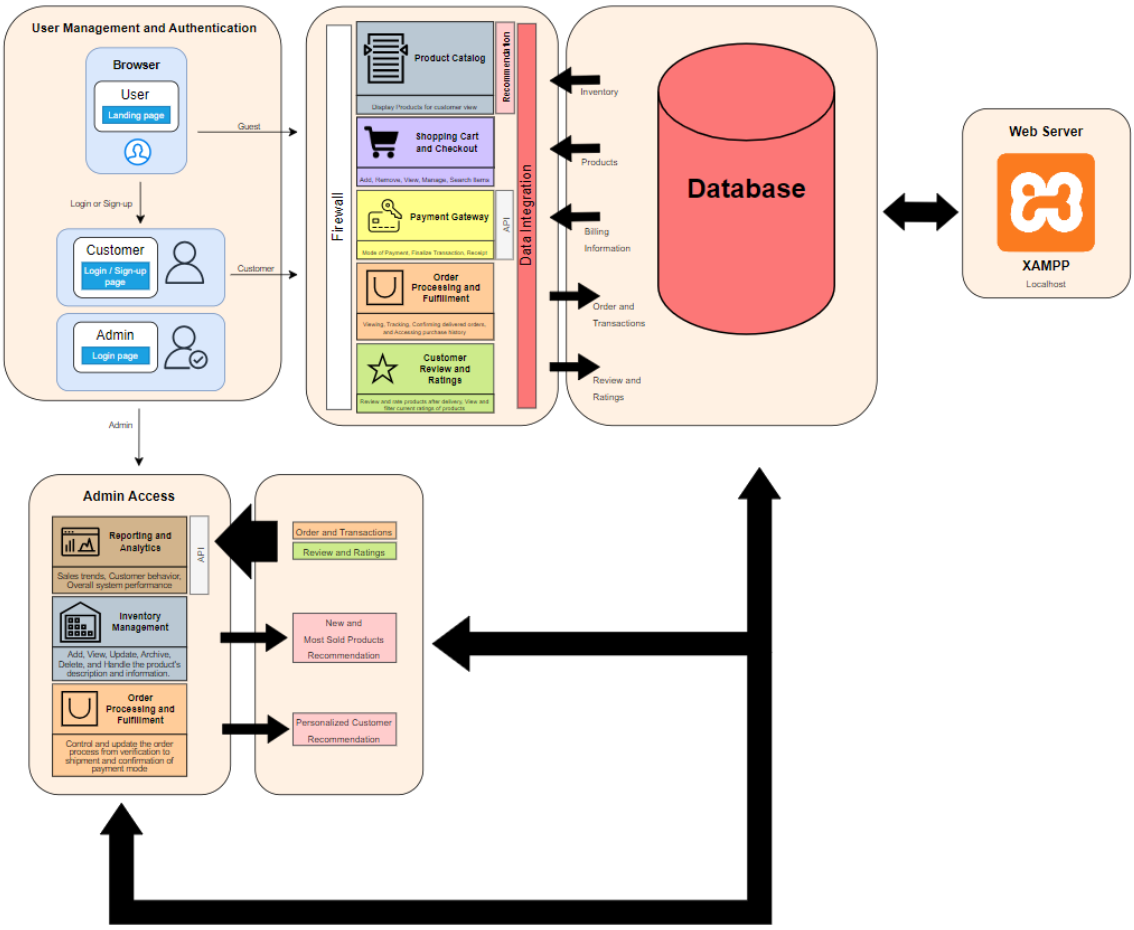
7. Recommendation Engine: The module utilizes algorithms to provide personalized product recommendations based on the user's purchase history by comparing the item to the other products offered in the system. In addition, it also recommends the newest and most sold products based on the inventory and orders fulfilled.

8. Reporting and Analytics: The module focuses on generating a comprehensive report and analysis to offer valuable insights into sales trends, customer behavior, and overall system performance. This includes sales reports, inventory and stock status, performance of products, and reports on return or refund to handle customer complaints effectively.

Overall, the E-Commerce System includes various types of data which are collected and stored in an integrated and centralized database and accessed through a localhost web server. This includes user profiles, product information, transaction details and order summaries, customer information and reviews. In summary, the system serves as a central and dynamic platform for providing a seamless and secure environment for online commerce. Its submodules and functionalities are dedicated to enhancing user experience for guests, customers, and employee administrators. The system's architecture and data management protocols prioritize efficiency in handling the requirements and needs of an e-commerce system.

6 System Environment

System Architecture



The following are the major activities for each of the E-Commerce System's submodule:

1. User Management and Authentication: The module handles user profiles and authentication processes, ensuring secure and dedicated access for guests, customers, and administrators. Individuals can opt to log in to their existing accounts, sign up for new accounts, or utilize the system as a guest.

2. Product Catalog and Inventory Management: The module efficiently organizes and presents products in the catalog for customer and guests to view, while also managing inventory levels to provide accurate product description, prices, and details. The inventory management administrator possesses the capability to add, view, update, archive, and delete products.

3. Order Processing and Fulfillment: The module facilitates listing, tracking, and updating of customer or guest-placed orders, providing transparency in the order process and status. It also includes the option to track the shipment, process and view the history of previous purchases. Admins can control and update the entire order process.

4. Shopping Cart and Checkout: This user-friendly module enhances the shopping experience by allowing users to add, remove, view, manage, and search for items in their personal charts. Furthermore, it enables guests or customers to efficiently checkout items, providing their desired address along with contact, address, and billing information.

5. Payment Gateway Integration: This module is held responsible for implementing a secure payment gateway within the system to enable smooth transactions between the customer and order process. Users can choose their desired payment method and upon completion, a receipt is generated.

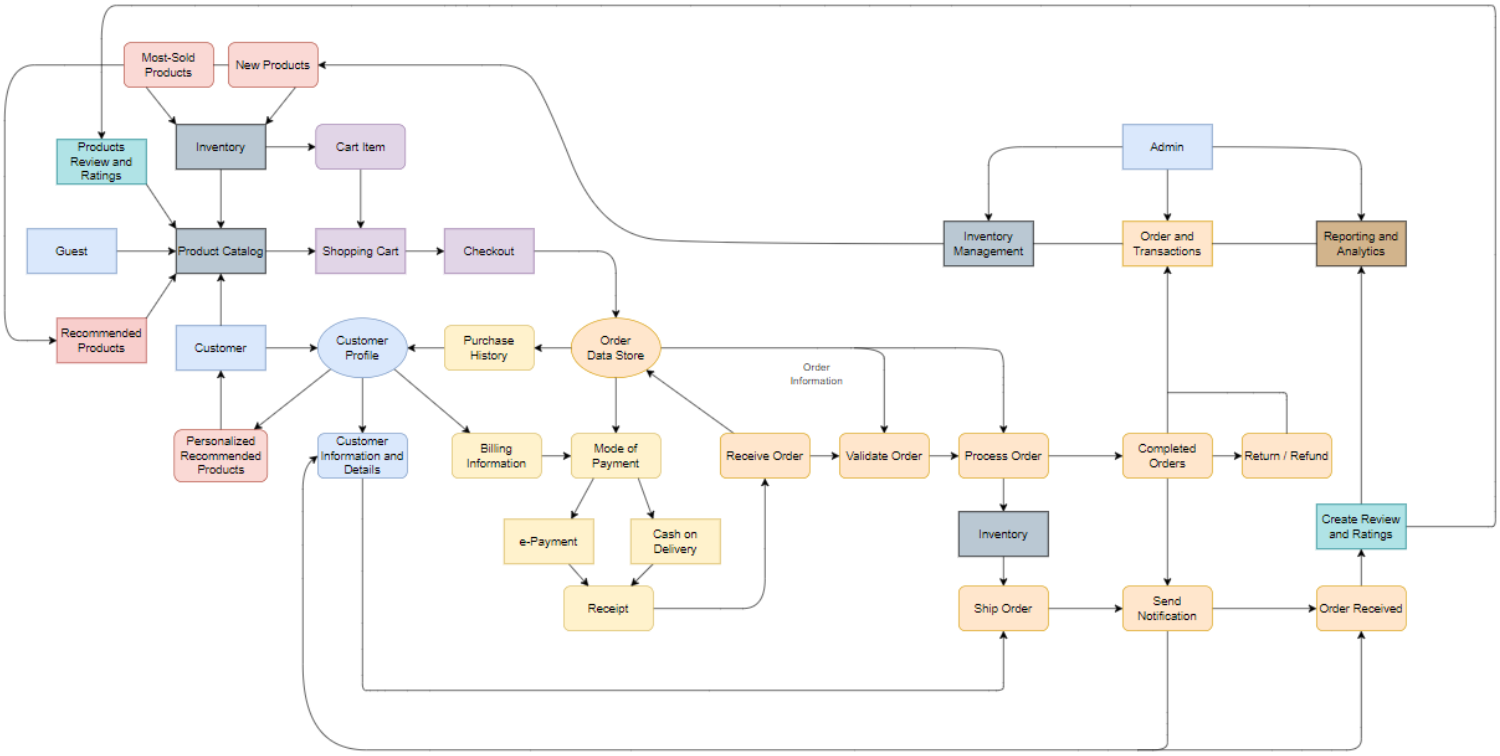
6. Customer Review and Ratings: This engaging module allows users to share insights through reviews and ratings. Users can view current reviews and ratings, employ filters based on the number of ratings, and express preferences by liking or disliking reviews to aid in content filtration. Users can contribute their own reviews by rating on a 1 to 5 scale after a specific item purchase.

7. Recommendation Engine: The module utilizes algorithms to provide personalized product recommendations based on a user's purchase history by comparing items to others in the system. It also recommends the newest and most sold products based on inventory and fulfilled orders.

8. Reporting and Analytics: The module is focused on generating comprehensive reports and analyses, it offers valuable insights into sales trends, customer behavior, and overall system performance. Reports include sales, inventory and stock status, product performance, and return or refund to attend to customer complaints.

7 System Interconnections/Information Sharing

Data Flow Diagram



8. Minimal Security Controls

These are the minimum required security controls to meet NATIONAL CYBERSECURITY PLAN 2023-2028. The control numbering below is consistent with NIST SP 800-171 (in the absence of details in the plan for Ph,

3.1 Access Control

3.1.1 Limit system access to authorized users, processes acting on behalf of authorized users, or devices (including other systems).

3.1.1	Control Summary Information
Responsible Role: Customer Reviews and Ratings	

Implementation Status (check all that apply):
☐ Implemented
☐ Partially implemented
☒ Planned
☐ Alternative implementation
☐ Not applicable

What is the solution and how is it implemented?
To address the requirement of limiting system access, organizations should implement robust access controls. This involves assigning unique user accounts, employing strong authentication mechanisms such as passwords or multi-factor authentication, and configuring permissions based on the principle of least privilege. Additionally, regularly review and update access permissions to ensure they align with the current organizational needs and personnel changes.

3.1.1	Control Summary Information

Responsible Role: Product Catalog and Inventory Management

Implementation Status (check all that apply):
- ☐ Implemented
- ☐ Partially implemented
- ☑ Planned
- ☐ Alternative implementation
- ☐ Not applicable

What is the solution and how is it implemented?
To limit system access to authorized users in an apparel e-commerce platform, create separate admin and customer accounts with distinct UIs.

3.1.1	Control Summary Information

Responsible Role: Reporting and Analytics

Implementation Status (check all that apply):
☐ Implemented
☐ Partially implemented
☒ Planned
☐ Alternative implementation
☐ Not applicable

What is the solution and how is it implemented?

The solution involves restricting system access to only authorized users, processes acting on behalf of authorized users, or authorized devices. This can be implemented through robust

authentication mechanisms, access control policies, and monitoring systems to ensure that only approved entities interact with the system.

3.1.1	Control Summary Information
Responsible Role: User Management and Authentication	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☑ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? - By implementing authentication methods, such as username/password or two-factor authentication, and employing access controls based on user permissions, the system ensures that only authorized users, processes, or devices, including other systems, have access.	

3.1.2 Limit system access to the types of transactions and functions that authorized users are permitted to execute

3.1.2	Control Summary Information
Responsible Role: User Management and Authentication	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☑ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? - By limiting system access to authorized transactions and functions by directly assigning and managing individual user permissions, ensuring that each user is granted access only to the specific transactions and functions they are permitted to execute.	

3.1.2	Control Summary Information
Responsible Role: Order Processing	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☒ Planned ☐ Alternative implementation ☐ Not applicable	

What is the solution and how is it implemented?

User account features are divided into two three types: User/ customer account, guest mode, and user administrator. Each has their own similarities and unique features. Particularly, there is a distinction between the customer and the administrator, whereas the administrator facilitates the processing of orders.

3.1.2	Control Summary Information

Responsible Role: Product Catalog and Inventory Management

Implementation Status (check all that apply):

- ☐ Implemented
- ☐ Partially implemented
- ☑ Planned
- ☐ Alternative implementation
- ☐ Not applicable

What is the solution and how is it implemented?

Limit user access to specific functionalities within the product catalog management submodule to enhance security and minimize unauthorized access to sensitive data.

3.1.3 Control the flow of Controlled Unclassified Information (CUI)in accordance with approved authorizations

3.1.3	Control Summary Information

Responsible Role:

Implementation Status (check all that apply):

☐ Implemented
☐ Partially implemented
☐ Planned
☐ Alternative implementation
☒ Not applicable

What is the solution and how is it implemented?

3.1.4 Separate the duties of individuals to reduce the risk of malevolent activity without collusion

3.1.4	Control Summary Information
Responsible Role: Order Processing	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☒ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? The order processing and fulfillment phase separate order workflow into a series of steps that do not overlap with one another. These steps include 1.) Checking Order Details, 2.) Packaging, 3.) Shipping, 4.) Delivery, 5.) Return process (situational), 6.) Updating database tables. The system will only proceed to the next step once the latter is accomplished. To prevent overlapping of tasks the system will undergo a series of conditional statements that check the status of the current process before proceeding to the next.	

3.1.5 Employ the principle of least privilege, including for specific security functions and privileged accounts

3.1.5	Control Summary Information
Responsible Role: Order Processing	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☒ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? The distinction between user account, guest mode, and administrator account limit permissions relative to the functions that each type could access. For instance, both guest and user accounts are granted the minimum permissions required to perform their specific job tasks (i.e., purchasing a product). This avoids providing excessive privileges that are unrelated to their responsibilities.	

3.1.6 Use non-privileged accounts or roles when accessing non-security functions

3.1.6	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☒ Not applicable	
What is the solution and how is it implemented?	

3.1.7 Prevent non-privileged users from executing privileged functions and audit the execution of such functions

3.1.7	Control Summary Information
Responsible Role: Order Processing	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☒ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? The interface for the user account/ guest and user admin will differ based on the needed functions of each individual. Both sides have access to the e-commerce website however, the Order Processing module will limit user/ guest access to only viewing the status of their order whereas, the administrative account is responsible for updating the order processing procedure, and securing communication for both the customer and the logistics partner/s.	

3.1.7	Control Summary Information
Responsible Role: Customer Reviews and Ratings	
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation	

☐ Not applicable
What is the solution and how is it implemented? To address the requirement of preventing non-privileged users from executing privileged functions and auditing such actions, organizations should enforce strict access controls to restrict user permissions. Privilege separation should be implemented to ensure that only authorized users have access to privileged functions. Simultaneously, enabling auditing features allows for the monitoring and recording of privileged function executions, aiding in the detection and investigation of potential security incidents.

3.1.7	Control Summary Information
Responsible Role: Reporting and Analytics	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☒ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? The solution involves implementing robust access controls to restrict non-privileged users from executing privileged functions in Reports and Analytics. Additionally, a comprehensive audit trail should be established to track and monitor the execution of privileged functions, ensuring accountability and security in the system.	

3.1.7	Control Summary Information
Responsible Role: User Management and Authentication	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☑ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? - By implementing stringent access controls and authorization checks within the system's code, non-privileged users can be prevented from executing privileged functions, and the execution of such functions can be audited through comprehensive logging mechanisms for later review and analysis.	

3.1.8 Limit unsuccessful login attempts

3.1.8	Control Summary Information
Responsible Role: User Management and Authentication	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☑ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? - By incorporating account lockout policies and rate-limiting mechanisms, you can limit unsuccessful login attempts, preventing potential unauthorized access by temporarily locking user accounts or introducing delays between consecutive login attempts.	

3.1.9 Provide privacy and security notices consistent with applicable CUI rules

3.1.9	Control Summary Information
Responsible Role: Payment Gateway Integration	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☒ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? It is planned that the user will be prompted whenever they confirm or enter transaction details	

3.1.9	Control Summary Information
Responsible Role: Shopping Cart and Checkout	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☒ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? Solution: The e-commerce system will implement a notification banner that displays the legal requirements of using the system before individuals log in to the system. The banner should inform the user that:	

1. The system is for authorized use only
2. The system may be monitored for security purposes
3. Unauthorized use may result in civil and criminal penalties
4. The user consents to these terms and conditions by using the system

The banner should be consistent with the applicable CUI rules. It will be displayed in every system that provides access to CUI, such as web servers, databases, and applications. It should be implemented using the appropriate configuration settings for the system, such as group policy, registry, or command line.

3.1.10 Use session lock with pattern-hiding displays to prevent access and viewing of data after period of inactivity

3.1.10	Control Summary Information
Responsible Role: Payment and Gateway Integration	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☒ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? This is planned to secure user authentications on transaction details, or passwords	

3.1.11 Terminate (automatically) a user session after a defined condition.

3.1.11	Control Summary Information
Responsible Role: Customer Reviews and Ratings	
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? The solution to automatically terminate user sessions after a defined condition involves implementing session timeout settings. Organizations can configure systems to log users out automatically after a specified period of inactivity, reducing the risk of unauthorized access in case users forget to log out manually. This security measure is typically managed through system or application settings, allowing administrators to define and enforce session timeout policies	

3.1.11	Control Summary Information
Responsible Role: User Management and Authentication	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☑ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? - By implementing session timeout settings, we can automatically terminate a user session after a defined condition, ensuring sessions expire after a specified period of inactivity and enhancing security and privacy.	

3.1.12 Monitor and control remote access sessions

3.1.12	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☒ Not applicable	
What is the solution and how is it implemented?	

3.1.13 Employ cryptographic mechanisms to protect the confidentiality of remote access sessions

3.1.13	Control Summary Information
Responsible Role: Payment and Gateway Integration	
Implementation Status (check all that apply): ☐ Implemented ☒ Partially implemented ☒ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? This is to ensure the safety of the transaction on the user's end, by protecting and authenticating certain functions such as checking if user is a bot	

3.1.14 Route remote access via managed access control points

3.1.14	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☒ Not applicable	
What is the solution and how is it implemented?	

3.1.15 Authorize remote execution of privileged commands and remote access to security-relevant information.

3.1.15	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☒ Not applicable	
What is the solution and how is it implemented?	

3.1.16 Authorize wireless access prior to allowing such connections

3.1.16	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☒ Not applicable	
What is the solution and how is it implemented?	

3.1.17 Protect wireless access using authentication and encryption

3.1.17	Control Summary Information

Responsible Role: Payment and Gateway Integration

Implementation Status (check all that apply):
☐ Implemented
☒ Partially implemented
☐ Planned
☐ Alternative implementation
☐ Not applicable

What is the solution and how is it implemented?
This is done to protect registered users on their data, by following guidelines from other submodules

3.1.17	Control Summary Information

Responsible Role: Shopping Cart and Checkout

Implementation Status (check all that apply):
☐ Implemented
☐ Partially implemented
☒ Planned
☐ Alternative implementation
☐ Not applicable

What is the solution and how is it implemented?

Solution:

1. Implement Wi-Fi Protected Access 2 or WPA3 encryption for the wireless network
    a. Configure the wireless routers and access points to use WPA2 or WPA3 encryption for the specific network used by the submodules to ensure that the data exchanged between other submodules is encrypted and secure.
2. Implement a firewall to control traffic between the shopping cart and checkout submodules.
    a. Configure the firewall to allow communication only on specific ports necessary for the submodule interaction. Block all other incoming and outgoing traffic by default.
3. Clearly define rules that allow communication between the shopping cart and checkout submodules
    a. Set up firewall rules to explicitly permit traffic between the IP addresses or ports associated with the submodules. Be specific about the nature of traffic that is allowed, and regularly review and update these rules as needed.

3.1.18 Control connection of mobile devices

3.1.18	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☒ Not applicable	
What is the solution and how is it implemented?	

3.1.19 Encrypt CUI on mobile devices and mobile computing platforms

3.1.19	Control Summary Information
Responsible Role: Payment Gateway Integration	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☒ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? This is to ensure data security, by following other submodules methods on encryption.	

3.1.20 Verify and control/limit connections to and use of external systems

3.1.20	Control Summary Information
Responsible Role: Customer Reviews and Ratings	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☒ Planned ☐ Alternative implementation ☐ Not applicable	

What is the solution and how is it implemented?
To verify and control/limit connections to and use of external systems, organizations should implement robust network access controls. This involves configuring firewalls, intrusion detection/prevention systems, and other security measures to monitor and restrict connections between internal systems and external networks, helping to prevent unauthorized access and potential security breaches.

3.1.20	Control Summary Information

Responsible Role: Payment Gateway Integration

Implementation Status (check all that apply):
☐ Implemented
☐ Partially implemented
☒ Planned
☐ Alternative implementation
☐ Not applicable

What is the solution and how is it implemented?
This is planned to reduce link of system to external services that may damage security and customer data integrity, by setting a limit on what third party applications may be used such as gcash

3.1.20	Control Summary Information

Responsible Role: Reporting and Analytics

Implementation Status (check all that apply):
☐ Implemented
☐ Partially implemented
☒ Planned
☐ Alternative implementation
☐ Not applicable

What is the solution and how is it implemented?

The solution involves implementing a secure gateway or firewall to verify and control connections to external systems in the context of Reports and Analytics. Access restrictions and usage limitations should be configured within the gateway to prevent unauthorized or excessive data exchange, ensuring a secure and controlled interaction with external systems.

3.1.21 Limit use of organizational portable storage devices on external systems

3.1.21	Control Summary Information

Responsible Role: Customer Reviews and Ratings
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☒ Planned ☐ Alternative implementation ☐ Not applicable
What is the solution and how is it implemented? To address the requirement of limiting the use of organizational portable storage devices on external systems, organizations should implement strict access controls and policies. This involves configuring systems to recognize and restrict the use of portable storage devices only to authorized internal systems, preventing potential data exposure and unauthorized access on external systems.

3.1.21	Control Summary Information
Responsible Role: Reporting and Analytics	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☒ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? The solution entails implementing endpoint security measures to restrict the use of organizational portable storage devices on external systems within the Reports and Analytics environment. This can be achieved by deploying endpoint security software that enforces policies to control and monitor the connection and usage of portable storage devices, enhancing data protection and mitigating potential security risks.	

3.1.22 Control CUI posted or processed on publicly accessible systems

3.1.22	Control Summary Information
Responsible Role: Customer Reviews and Ratings	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☒ Planned ☐ Alternative implementation ☐ Not applicable	

What is the solution and how is it implemented? To control Controlled Unclassified Information (CUI) posted or processed on publicly accessible systems, organizations should implement access controls and encryption measures. This involves configuring systems to restrict access to authorized users only, employing encryption to protect the confidentiality of CUI during processing and transmission, and regularly monitoring and auditing these systems to ensure compliance with security policies.

3.1.22	Control Summary Information
Responsible Role: Reporting and Analytics	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☒ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? The solution involves implementing access controls and encryption measures to control Controlled Unclassified Information (CUI) posted or processed on publicly accessible systems within the Reports and Analytics environment. Utilizing role-based access controls and employing encryption protocols for data in transit and at rest helps safeguard sensitive information from unauthorized access and ensures compliance with security standards.	

3.2 Awareness and Training

3.2.1 Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems

3.2.1	Control Summary Information
Responsible Role: Customer Reviews and Ratings	
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	

What is the solution and how is it implemented? To address the requirement of ensuring awareness of security risks and policies, organizations should implement a comprehensive communication strategy. This involves regularly disseminating information to managers, systems administrators, and users regarding the specific security risks associated with their activities, as well as educating them on applicable policies, standards, and procedures. This communication strategy may include training sessions, newsletters, and periodic reminders to reinforce a culture of security awareness within the organization.

3.2.1	Control Summary Information
Responsible Role: Payment and Gateway Integration	
Implementation Status (check all that apply): ☐ Implemented ☒ Partially implemented ☒ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? This is planned because it is the bare minimum of safety and security awareness and is discussed among the developers of the whole system	

3.2.2 Ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

3.2.2	Control Summary Information
Responsible Role: Customer Reviews and Ratings	
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	

What is the solution and how is it implemented?
The solution to ensuring that organizational personnel are adequately trained for their information security-related duties involves implementing a structured training program. This includes creating and delivering training modules tailored to employees' specific roles and responsibilities, covering essential aspects of information security to enhance their knowledge and skills in safeguarding organizational assets and data. Regular updates and assessments should be incorporated to keep personnel informed about evolving security threats and best practices.

3.2.2	Control Summary Information

Responsible Role: Payment and Gateway Integration

Implementation Status (check all that apply):
☐ Implemented
☒ Partially implemented
☒ Planned
☐ Alternative implementation
☐ Not applicable

What is the solution and how is it implemented?
This is planned because it is the bare minimum of safety and security awareness and is discussed among the developers of the whole system

3.2.2	Control Summary Information

Responsible Role: Order Processing

Implementation Status (check all that apply):
☐ Implemented
☐ Partially implemented
☒ Planned
☐ Alternative implementation
☐ Not applicable

What is the solution and how is it implemented?

The user administrator should be familiarized with the system's features and capabilities to ensure a smooth systematic order processing procedure. Therefore in a realistic setting, the administrative staff (the seller) must be well-informed of the order processing sub-modules protocols through tutorial or by developing a user manual.

3.2.3 Provide security awareness training on recognizing and reporting potential indicators of insider threat

3.2.3	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? To fulfill the requirement of providing security awareness training on recognizing and reporting potential indicators of insider threat, organizations should implement regular training programs for employees. This involves educating personnel about the signs of insider threats, emphasizing the importance of vigilance, and establishing clear reporting mechanisms to ensure timely identification and mitigation of potential risks.	

3.2.3	Control Summary Information
Responsible Role: Payment and Gateway Integration	
Implementation Status (check all that apply): ☐ Implemented ☒ Partially implemented ☒ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? This is planned because it is the bare minimum of safety and security awareness and is discussed among the developers of the whole system	

3.3 Audit and Accountability

3.3.1 Create, protect, and retain system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate system activity

3.3.1	Control Summary Information
Responsible Role: Payment and Gateway Integration	

Implementation Status (check all that apply):
☐ Implemented
☒ Partially implemented
☒ Planned
☐ Alternative implementation
☐ Not applicable

What is the solution and how is it implemented?
This is planned because it is mandatory that there is an auditing process not only for the user but also for the administrators and is discussed among the developers of the whole system

3.3.1	Control Summary Information

Responsible Role: Order Processing

Implementation Status (check all that apply):
☐ Implemented
☐ Partially implemented
☒ Planned
☐ Alternative implementation
☐ Not applicable

What is the solution and how is it implemented?

A logging system in the order processing sub-module will be implemented to keep records of previous purchases and ensure transparency between the customer (user) and the seller (user admin). This will be implemented as a feature for both types of users. An additional feature for the user admin unlocks the ability to view the history of all purchased products for record and reporting.

3.3.1	Control Summary Information

Responsible Role: Product Catalog and Inventory Management

Implementation Status (check all that apply):
☐ Implemented
☐ Partially implemented
☑ Planned
☐ Alternative implementation
☐ Not applicable

What is the solution and how is it implemented?

3.3.1	Control Summary Information
To track and analyze system activity, create, protect, and retain audit records for product catalog admin authorization. This includes recording admin actions like creating, editing, and deleting products, as well as adding or removing inventory. Audit records should be protected from unauthorized access and maintained for an appropriate period of time	

3.3.2 Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions

3.3.2	Control Summary Information
Responsible Role: Payment and Gateway Integration	
Implementation Status (check all that apply): ☐ Implemented ☒ Partially implemented ☒ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? Tracing the users of their actions proves useful not only for the user's end on tracking transactions but also for safety measures for niche situations regarding transactions, fraud, fake accounts, etc.	

3.3.2	Control Summary Information
Responsible Role: Order Processing	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☒ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? The logging system enables the user to view records of past orders. In the given scenario, the logging system facilitates user accountability by allowing users to view records of past orders. Each time a user accesses the system to view past orders, a log entry is generated, capturing details such as the user's identifier, the specific action (viewing records), the timestamp, and any relevant details about the orders viewed. Continued implementation involves regularly reviewing these logs to ensure that access is legitimate and aligns with user roles and permissions.	

3.3.2	Control Summary Information
Responsible Role: Product Catalog and Inventory Management	
Implementation Status (check all that apply): ☑ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? The admin user can be traced by the user info that has been used to login and update at a time in the database what specific or update did the user do during the session of product catalog.	

3.3.3 Review and update audited events

3.3.3	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☒ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? This is just within the boundary of the scope, and will be implemented partially to help other submodules review the cases of auditing	

3.3.4 Alert in the event of an audit process failure

3.3.4	Control Summary Information
Responsible Role: Payment and Gateway Integration	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☒ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? There will be notification for the administrators in case of process failure	

3.3.4	Control Summary Information
Responsible Role: Product Catalog and Inventory Management	
Implementation Status (check all that apply): ☑ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? The admin user can be alerted by the user info that has been used to login and update at a time in the database what specific or update did the user do during the session of the product catalog.	

3.3.5 Correlate audit review, analysis, and reporting processes for investigation and response to indications of inappropriate, suspicious, or unusual activity

3.3.5	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☒ Not applicable	
What is the solution and how is it implemented?	

3.3.6 Provide audit reduction and report generation to support on-demand analysis and reporting

3.3.6	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☒ Not applicable	
What is the solution and how is it implemented?	

3.3.6	Control Summary Information

3.3.7 Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records

3.3.7	Control Summary Information
Responsible Role: Payment and Gateway Integration	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☒ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? There will be a record for computing and generating process	

3.3.8 Protect audit information and audit tools from unauthorized access, modification, and deletion

3.3.8	Control Summary Information
Responsible Role: Payment and Gateway Integration	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☒ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? There will be security functions that are only available for back-end users	

3.3.8	Control Summary Information
Responsible Role: Product Catalog and Inventory Management	
Implementation Status (check all that apply): ☑ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation	

3.3.8	Control Summary Information

☐ Not applicable

What is the solution and how is it implemented?

Unauthorized accounts cannot access the audit tools to audit information history by different users.

3.3.8	Control Summary Information

Responsible Role: Shopping Cart and Checkout

Implementation Status (check all that apply):

☐ Implemented

☐ Partially implemented

☒ Planned

☐ Alternative implementation

☐ Not applicable

What is the solution and how is it implemented?

Solution:

1. Implement logging and monitoring to detect and respond to unauthorized access attempts.
    a. Use log analysis tools like Monolog to monitor access to audit info and set up alerts for suspicious activities.
2. Implement a backup and recovery plan to prevent data loss in case of unauthorized deletion or modification
    a. Regularly backup audit information and tools, and test the restoration process to ensure that data can be recovered in the event of a security incident.
3. Ensure that the development of the shopping cart and checkout module follows secure coding practices
    a. Conduct security reviews during the development process to identify and address security vulnerabilities. Use secure coding guidelines and perform regular code reviews.

3.3.9 Limit management of audit functionality to a subset of privileged users

3.3.9	Control Summary Information

Responsible Role: Shopping Cart and Checkout

Implementation Status (check all that apply):

☐ Implemented

☐ Partially implemented

☒ Planned

☐ Alternative implementation

☐ Not applicable
What is the solution and how is it implemented? Solution: 1. Set up access controls to restrict who can view, modify, or delete audit information and tools a. Implement access control lists (ACLs) and permissions to limit access to sensitive data. Regularly review and update access controls based on changes in personnel or roles.

3.3.9	Control Summary Information
Responsible Role: Product Catalog and Inventory Management	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☑ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? Product Catalog Admins possess the authority to grant and revoke access to various user accounts, ensuring the security and integrity of stored information.	

3.4 Configuration Management

3.4.1 Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles

3.4.1	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☒ Not applicable	
What is the solution and how is it implemented?	

3.4.2 Establish and enforce security configuration settings for information technology products employed in organizational systems

3.4.2	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☒ Not applicable	
What is the solution and how is it implemented?	

3.4.3 Track, review, approve/disapprove, and audit changes to organizational systems

3.4.3	Control Summary Information
Responsible Role: Payment and Gateway Integration	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☒ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? There will be logs for any changes to organizational system	

3.4.3	Control Summary Information
Responsible Role: Product Catalog and Inventory Management	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☑ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? To manage system changes effectively, implement a comprehensive process that tracks, reviews, approves/disapproves, and audits changes. This helps maintain data integrity,	

3.4.3	Control Summary Information
enhance security, and simplify compliance. The product catalog admin can Define roles, establish procedures, utilize tools, provide training, and continuously monitor the process.	

3.4.4 Analyze the security impact of changes prior to implementation

3.4.4	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☒ Not applicable	
What is the solution and how is it implemented?	

3.4.5 Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems

3.4.5	Control Summary Information
Responsible Role: Order Processing	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☒ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? Given that the user administrator has the capability to update the status of the tracked order, a security measure must ensure that the order is tracked correctly and therefore, the sub-module restricts accidental changes within the order tracking phase to correct the order tracking process. This is implemented through conditional measures and/or confirmation messages before imposing changes or updates.	

3.4.5	Control Summary Information
Responsible Role: Shopping Cart and Checkout	

Implementation Status (check all that apply):

☐ Implemented

☐ Partially implemented

☒ Planned

☐ Alternative implementation

☐ Not applicable

What is the solution and how is it implemented?

Solution:

1. Create an inventory of all installed programs, open ports, enabled protocols, and running services on your system.
    a. Use automated tools for system scanning and inventory.
    b. Regularly review and update the inventory to reflect changes.
2. Clearly define and document the essential programs, functions, ports, protocols, and services required for the proper functioning of the system.
    a. Collaborate with system administrators, developers, and other stakeholders to determine essential services.
    b. Document the purpose and business justification for each essential service.
3. Implement application whitelisting to allow only authorized and essential programs to run.
    a. Deploy application control tools that support whitelisting and blacklisting.
    b. Regularly review and update the whitelist and blacklist.

3.4.6 Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities

3.4.6	Control Summary Information

Responsible Role: Product Catalog and Inventory Management

Implementation Status (check all that apply):

☐ Implemented

☐ Partially implemented

☑ Planned

☐ Alternative implementation

☐ Not applicable

What is the solution and how is it implemented?

The system will provide a detailed instruction of each functionality in the system if they need a guide of what is the use of each of the functions in the admin and customer system.

3.4.7 Restrict, disable, and prevent the use of nonessential programs, functions, ports, protocols, and services

3.4.7	Control Summary Information
Responsible Role: Shopping Cart and Checkout	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☒ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? Solution: 1. Identifying nonessential programs and functions that are not crucial for the shopping cart and checkout processes. a. Disable or remove unnecessary programs or functionalities from the system to minimize potential vulnerabilities. 2. Close or restrict access to ports and protocols that are not required for the shopping cart and checkout functionalities. a. Configure firewalls or network settings to block unnecessary ports and protocols, reducing the potential attack surface. 3. Disable or deactivate services that are not directly related to the shopping cart and checkout operations. a. Reviewing and managing background services running on the system, ensuring only essential services are active.	

3.4.8 Apply deny-by-exception (blacklist) policy to prevent the use of unauthorized software or denyall, permit-by-exception (whitelisting) policy to allow the execution of authorized software

3.4.8	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☒ Not applicable	
What is the solution and how is it implemented?	

3.4.9 Control and monitor user-installed software

3.4.9	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☒ Not applicable	
What is the solution and how is it implemented?	

3.5 Identification and Authentication

3.5.1 Identify system users, processes acting on behalf of users, or devices

3.5.1	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☒ Not applicable	
What is the solution and how is it implemented?	

3.5.2 Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational systems

3.5.2	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☒ Not applicable	
What is the solution and how is it implemented?	

3.5.2	Control Summary Information

3.5.3 Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts

3.5.3	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☒ Not applicable	
What is the solution and how is it implemented?	

3.5.4 Employ replay-resistant authentication mechanisms for network access to privileged and nonprivileged accounts

3.5.4	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☒ Not applicable	
What is the solution and how is it implemented?	

3.5.5 Prevent reuse of identifiers for a defined period

3.5.5	Control Summary Information
Responsible Role: Product Catalog and Inventory Management	
Implementation Status (check all that apply): ☑ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation	

3.5.5	Control Summary Information

☐ Not applicable

What is the solution and how is it implemented?

1. Maintain a retired identifier list: Create a database or data structure to store retired identifiers.
2. Validate new identifiers: Before assigning a new identifier, check if it exists in the retired identifier list. If it does, generate a new identifier until a unique one is found.
3. Define the retirement period: Determine the appropriate timeframe for preventing identifier reuse. This could be the product's lifecycle, a fixed period, or a combination of both.
4. Implement identifier generation policies: Establish clear rules for generating unique identifiers, considering factors like identifier length, format, and potential for collisions.
5. Automate identifier management: Utilize automated processes to manage the retired identifier list, identifier validation, and generation.

3.5.6 Disable identifiers after a defined period of inactivity

3.5.6	Control Summary Information

Responsible Role:

Implementation Status (check all that apply):
☐ Implemented
☐ Partially implemented
☐ Planned
☐ Alternative implementation
☒ Not applicable

What is the solution and how is it implemented?

3.5.7 Enforce a minimum password complexity and change of characters when new passwords are created

3.5.7	Control Summary Information

Responsible Role:

Implementation Status (check all that apply):
☐ Implemented
☐ Partially implemented
☐ Planned

3.5.7	Control Summary Information
☐ Alternative implementation ☒ Not applicable	
What is the solution and how is it implemented?	

3.5.8 Prohibit password reuse for a specified number of generations

3.5.8	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☒ Not applicable	
What is the solution and how is it implemented?	

3.5.9 Allow temporary password use for system logons with an immediate change to a permanent password

3.5.9	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☒ Not applicable	
What is the solution and how is it implemented?	

3.5.10 Store and transmit only cryptographically-protected passwords

3.5.10	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented	

3.5.10	Control Summary Information

☐ Partially implemented
☐ Planned
☐ Alternative implementation
☒ Not applicable

What is the solution and how is it implemented?

3.5.11 Obscure feedback of authentication information

3.5.11	Control Summary Information

Responsible Role:

Implementation Status (check all that apply):
☐ Implemented
☐ Partially implemented
☐ Planned
☐ Alternative implementation
☒ Not applicable

What is the solution and how is it implemented?

3.6 Incident Response

3.6.1 Establish an operational incident-handling capability for organizational systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities

3.6.1	Control Summary Information

Responsible Role: Customer Reviews and Ratings

Implementation Status (check all that apply):
☒ Implemented
☐ Partially implemented
☐ Planned
☐ Alternative implementation
☐ Not applicable

What is the solution and how is it implemented To meet the requirement of establishing an operational incident-handling capability, organizations should develop a comprehensive incident response plan covering preparation, detection, analysis, containment, recovery, and user response activities. Implementation involves defining clear procedures, assigning responsibilities, conducting regular training, and establishing communication protocols to ensure an effective and coordinated response to security incidents in organizational systems.

3.6.2 Track, document, and report incidents to appropriate officials and/or authorities both internal and external to the organization

3.6.2	Control Summary Information
Responsible Role: Payment Gateway Integration	
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? Implement a dedicated incident tracking system or use a comprehensive ticketing platform to document and categorize incidents. Establish a clear internal reporting process and define escalation procedures. Ensure compliance with legal and regulatory requirements and establish communication protocols for reporting incidents to external authorities when necessary.	

3.6.3 Test the organizational incident response capability.

3.6.3	Control Summary Information
Responsible Role: Customer Reviews and Ratings	
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	

What is the solution and how is it implemented?
The solution to testing the organizational incident response capability involves conducting regular and realistic simulations of potential security incidents. This is implemented by designing and executing scenarios that mimic various cyber threats, enabling the organization to evaluate and enhance its incident response procedures, identify weaknesses, and improve overall preparedness.

3.6.3	Control Summary Information

Responsible Role: Payment Gateway Integration

Implementation Status (check all that apply):
☐ Implemented
☐ Partially implemented
☒ Planned
☐ Alternative implementation
☐ Not applicable

What is the solution and how is it implemented?
There will be testing for the quality of the capabilities of the system to test out the response incase of emergencies.

3.6.3	Control Summary Information

Responsible Role: Recommendation Engine (applicable for Information Security Office)

Implementation Status (check all that apply):
☐ Implemented
☐ Partially implemented
☒ Planned
☐ Alternative implementation
☐ Not applicable

What is the solution and how is it implemented?
By conducting testing for security incidents to ensure that the recommendation module is responsive.

3.7 Maintenance

3.7.1 Perform maintenance on organizational systems

3.7.1	Control Summary Information

Responsible Role: Payment Gateway Integration

Implementation Status (check all that apply):
☐ Implemented
☐ Partially implemented
☒ Planned
☐ Alternative implementation
☐ Not applicable

What is the solution and how is it implemented?
There will be maintenance to make sure the system works and ensure data integrity.

3.7.1	Control Summary Information

Responsible Role: Recommendation Engine

Implementation Status (check all that apply):
☐ Implemented
☐ Partially implemented
☒ Planned
☐ Alternative implementation
☐ Not applicable

What is the solution and how is it implemented?
The solution is to keep the system up to date and secure by implementing a system maintenance plan.

3.7.1	Control Summary Information

Responsible Role: Product Catalog and Inventory Management

Implementation Status (check all that apply):
☑ Implemented
☐ Partially implemented
☐ Planned
☐ Alternative implementation
☐ Not applicable

What is the solution and how is it implemented?

To maintain system performance, security and compliance, perform regular maintenance by conducting preventive scans, corrective measures, and adaptive updates.

3.7.2 Provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance

3.7.2	Control Summary Information
Responsible Role: Payment and Gateway Integration	
Implementation Status (check all that apply): ☐ Implemented ☒ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? There will be a separate side for admins to control the system.	

3.7.2	Control Summary Information
Responsible Role: Recommendation Engine	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☒ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? Effective controls can be promoted by providing access controls, logging, and monitoring protocols.	

3.7.3 Ensure equipment removed for off-site maintenance is sanitized of any CUI

3.7.3	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☒ Not applicable	
What is the solution and how is it implemented?	

3.7.4 Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems

3.7.4	Control Summary Information
Responsible Role: Payment Gateway Integration	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☒ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? The admins will make sure to checkout any updates that will be implemented during maintenance hours	

3.7.4	Control Summary Information
Responsible Role: Order Processing	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☒ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? For best practice, it is encouraged that the media used in launching the system should be checked as well as ensure that the system's code structure is well within the parameters of a secured software standard. As such, devices shall be carefully considered before using.	

3.7.5 Require multi factor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete

3.7.5	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☒ Not applicable	

3.7.5	Control Summary Information
What is the solution and how is it implemented?	

3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization.

3.7.6	Control Summary Information
Responsible Role: Payment Gateway Integration	
Implementation Status (check all that apply): ☐ Implemented ☒ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? Managers and Team leaders will ensure that there will be supervision on personnel with low authority access to the system.	

3.8 Media Protection

3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital

3.8.1	Control Summary Information
Responsible Role: Payment Gateway Integration	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☒ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? Administrators will ensure that securing media containing CUI are properly secured.	

3.8.1	Control Summary Information
Responsible Role: Product Catalog and Inventory Management	

3.8.1	Control Summary Information

Implementation Status (check all that apply):

- ☑ Implemented
- ☐ Partially implemented
- ☐ Planned
- ☐ Alternative implementation
- ☐ Not applicable

What is the solution and how is it implemented?

Implement physical and logical security measures to protect system media containing CUI.

Physical Control:

- Store physical media in secure locations with restricted access.
- Implement tracking and check-out procedures for physical media.

Logical Protection:

- Encrypt digital media using strong encryption algorithms.
- Implement access controls based on user roles and permissions.
- Use secure communication channels for data transfer.

General Precautions:

- Clearly label physical media as containing CUI.
- Properly dispose of physical media when no longer needed.
- Provide training on CUI handling procedures and security protocols.

3.8.2 Limit access to CUI on system media to authorized users

3.8.2	Control Summary Information

Responsible Role: Customer Reviews and Ratings

Implementation Status (check all that apply):

☐ Implemented
☐ Partially implemented
☒ Planned
☐ Alternative implementation
☐ Not applicable

What is the solution and how is it implemented?
To address the requirement of limiting access to Controlled Unclassified Information (CUI) on system media, organizations should enforce access controls and permissions. This is implemented by configuring the system to grant access only to authorized users, ensuring that sensitive information stored on media is restricted to individuals with the necessary permissions.

3.8.2	Control Summary Information
Responsible Role: Payment Gateway Integration	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☒ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? There will be different levels of administrators to make sure that project managers can oversee members' ideas.	

3.8.2	Control Summary Information
Responsible Role: Project Manager	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☒ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? The solution involves implementing access controls and encryption mechanisms for system media storing Controlled Unclassified Information (CUI) within the e-commerce report and analytics environment. This includes employing file-level encryption and strict access permissions, ensuring that only authorized users with specific credentials can access and modify CUI stored on the system media.	

3.8.3 Sanitize or destroy system media containing CUI before disposal or release for reuse

3.8.3	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☒ Not applicable	
What is the solution and how is it implemented?	

3.8.4 Mark media with necessary CUI markings and distribution limitations

3.8.4	Control Summary Information
Responsible Role: Payment Gateway Integration	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☒ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented?	

3.8.5 Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas

3.8.5	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☒ Not applicable	
What is the solution and how is it implemented?	

3.8.6 Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards

3.8.6	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☒ Not applicable	
What is the solution and how is it implemented?	

3.8.6	Control Summary Information

3.8.7 Control the use of removable media on system components

3.8.7	Control Summary Information
Responsible Role: Payment Gateway Integration	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☒ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? The administrators will make sure that there will be supervisions regarding the use of removable media on system components	

3.8.8 Prohibit the use of portable storage devices when such devices have no identifiable owner

3.8.8	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☒ Not applicable	
What is the solution and how is it implemented?	

3.8.9 Protect the confidentiality of backup CUI at storage locations.

3.8.9	Control Summary Information
Responsible Role: Payment and Gateway Integration	

Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☒ Planned ☐ Alternative implementation ☐ Not applicable
What is the solution and how is it implemented? There will be a backup database for the system.

3.8.9	Control Summary Information
Responsible Role: Recommendation Engine	
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? Confidentiality can be promoted by encrypting the data, storing it to a secure database, and controlling access to the database.	

3.9 Personnel Security

3.9.1 Screen individuals prior to authorizing access to organizational systems containing CUI.

3.9.1	Control Summary Information
Responsible Role: Customer Reviews and Ratings	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☒ Planned ☐ Alternative implementation ☐ Not applicable	

What is the solution and how is it implemented? to screen individuals prior to authorizing access to organizational systems containing Controlled Unclassified Information (CUI) involves implementing thorough identity verification processes. This may include background checks, credential validation, and verification of the individual's need for access. Access should only be granted to those who meet the defined criteria, ensuring a secure and controlled environment for handling sensitive information.

3.9.2 Ensure that CUI and organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers

3.9.2	Control Summary Information
Responsible Role: Payment Gateway Integration	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☒ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? There will be supervisions for authorized users	

3.10 Physical Protection

3.10.1 Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.

3.10.1	Control Summary Information
Responsible Role: Payment Gateway Integration	
Implementation Status (check all that apply): ☐ Implemented ☒ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented?	

3.10.1	Control Summary Information
Responsible Role: Product Catalog and Inventory Management	
Implementation Status (check all that apply): ☑ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? Implement physical access control measures to restrict access to authorized personnel only. ● Identify Access Requirements ● Secure Physical Spaces ● Implement Access Control Systems ● Establish Visitor Management Procedures ● Monitor and Audit Access ● Educate and Train Employees	

3.10.2 Protect and monitor the physical facility and support infrastructure for organizational systems

3.10.2	Control Summary Information
Responsible Role: Payment Gateway Integration	
Implementation Status (check all that apply): ☐ Implemented ☒ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? There will be maintenance security for the facility and infrastructure	

3.10.3 Escort visitors and monitor visitor activity

3.10.3	Control Summary Information
Responsible Role: Payment Gateway Integration	

Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☒ Planned ☐ Alternative implementation ☐ Not applicable
What is the solution and how is it implemented? There will be supervisions regarding unauthorized users and will be limited to what they can access

3.10.3	Control Summary Information
Responsible Role: Recommendation Engine	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☒ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? The recommendation module can escort guests and monitor visitor activity while they are browsing. Monitoring their movements like browsing.	

3.10.4 Maintain audit logs of physical access

3.10.4	Control Summary Information
Responsible Role: Payment Gateway Integration	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☒ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? There will be tagging for users physical access of audit logs.	

3.10.4	Control Summary Information
Responsible Role: Order Processing	

Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☒ Planned ☐ Alternative implementation ☐ Not applicable
What is the solution and how is it implemented? The logging system shall include the history of the order, including customer information and the date of which the order was processed and delivered. This is to keep the record of purchase for future references.

3.10.5 Control and manage physical access devices

3.10.5	Control Summary Information
Responsible Role: Payment and Gateway Integration	
Implementation Status (check all that apply): ☐ Implemented ☒ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? Manage users' access in the system.	

3.10.6 Enforce safeguarding measures for CUI at alternate work sites (e.g., telework sites).

3.10.6	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☒ Not applicable	
What is the solution and how is it implemented?	

3.11 Risk Assessment

3.11.1 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI

3.11.1	Control Summary Information
Responsible Role: Payment Gateway Integration	
Implementation Status (check all that apply): ☐ Implemented ☒ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? There will be maintenance for operations in the system.	

3.11.1	Control Summary Information
Responsible Role: Product Catalog and Inventory Security Plan	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☑ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? The Product Catalog admin can provide a periodically assess of the items that are being sold in the store with the provided guidelines and roles.	

3.11.2 Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified

3.11.2	Control Summary Information
Responsible Role: Payment Gateway Integration	

Implementation Status (check all that apply): ☐ Implemented ☒ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable
What is the solution and how is it implemented? There will be maintenance for checking vulnerability within the system.

3.11.3 Remediate vulnerabilities in accordance with assessments of risk.

3.11.3	Control Summary Information
Responsible Role: Payment Gateway Integration	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☒ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? There will be an matrix guide on how to handle different level of risks	

3.12 Security Assessment

3.12.1 Periodically assess the security controls in organizational systems to determine if the controls are effective in their application

3.12.1	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☒ Not applicable	
What is the solution and how is it implemented?	

3.12.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems

3.12.2	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☒ Not applicable	
What is the solution and how is it implemented?	

3.12.3 Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls

3.12.3	Control Summary Information
Responsible Role: Recommendation Engine	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☒ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? To effectively monitor the security controls on a timely basis that is implemented in the system to ensure the data protection and integrity, and its effectiveness in the engine.	

3.12.3	Control Summary Information
Responsible Role: Payment Gateway Integration	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☒ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? There will be maintenance for confirmation of any process within the submodule of payment gateway	

3.12.4 Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.

3.12.4	Control Summary Information
Responsible Role: Recommendation Engine	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☒ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? The system security plans that are going to be implemented onto the engine will be continuously monitored, developed, and documented.	

3.12.4	Control Summary Information
Responsible Role: Order Processing	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☒ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? The order processing sub-module shall update the security plan as needed. This will need adjusting depending on how the system will behave during the testing stage. The sub-module shall implement adjustments, and updates once a bug or a lack of requirement compliance has been identified along the way.	

3.12.4	Control Summary Information
Responsible Role: Payment Gateway Integration	

Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☒ Planned ☐ Alternative implementation ☐ Not applicable
What is the solution and how is it implemented? There will be continuous update with the integration of other submodules and APIs

3.13 System and Communications Protection

3.13.1 Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems

3.13.1	Control Summary Information
Responsible Role: Order Processing	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☒ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? It is within the scope of the order processing sub-module to update the logistics partner and customer through a communication line (via chat or utilization of contact information provided). The communication between entities must be based on tracking the order's status. Therefore, the system shall provide a close to real-time update on order status (as controlled by the user administrator).	

3.13.2 Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems

3.13.2	Control Summary Information
Responsible Role: Customer Reviews and Ratings	

Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable
What is the solution and how is it implemented? integrate secure architectural designs, follow secure software development methodologies like DevSecOps, and apply systems engineering principles to embed robust information security practices within the infrastructure and development lifecycle of the Customer Reviews and Ratings system.

3.13.2	Control Summary Information
Responsible Role: Recommendation Engine	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☒ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? Such designs, techniques, and principles will be implemented onto the development of the recommendation engine within mind.	

3.13.2	Control Summary Information
Responsible Role: Order Processing	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☒ Planned ☐ Alternative implementation ☐ Not applicable	

What is the solution and how is it implemented?

The order processing sub-module shall employ development techniques such as an object-oriented paradigm that uses encapsulation and inheritance methods to improve coding efficiency, readability, and security. The code structure of the order processing module is crucial in system maintainability and reliability as future updates, and maintenance could be done accordingly.

3.13.2	Control Summary Information

Responsible Role: Reporting and Analytic

Implementation Status (check all that apply):
☐ Implemented
☐ Partially implemented
☒ Planned
☐ Alternative implementation
☐ Not applicable

What is the solution and how is it implemented?
The solution involves adopting a secure software development life cycle (SDLC) that integrates security measures at every stage, utilizing techniques like threat modeling, code reviews, and regular security testing within the e-commerce report and analytics systems. Additionally, employing architectural patterns that incorporate security by design, such as microservices with isolated security domains or containerization with strict access controls, helps fortify the overall information security posture.

3.13.2	Control Summary Information

Responsible Role: Product Catalog and Inventory Management

Implementation Status (check all that apply):
☐ Implemented
☐ Partially implemented
☑ Planned
☐ Alternative implementation
☐ Not applicable

What is the solution and how is it implemented?
The Product Catalog System will use the employed architectural design and software development to ensure the range and scope of each user who will use the system.

3.13.2	Control Summary Information
Responsible Role: Payment Gateway Integration	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☒ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? There will be blueprints for the whole submodule payment gateway integration	

3.13.3 Separate user functionality from system management functionality

3.13.3	Control Summary Information
Responsible Role: Order Processing	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☒ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? The user account and the administrative account will share similar interfaces but ultimately different functions. The system will not overlap with the two accounts as the user account can only access user features and the administrative account can only access administrative features. This is done through a separate interface once the user opts to log in.	

3.13.3	Control Summary Information
Responsible Role: Customer Reviews and Ratings	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☒ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented?	

creating distinct user roles with restricted access privileges and implementing role-based access controls to separate user interactions from system management functionalities within the Customer Reviews and Ratings system.

3.13.3	Control Summary Information
Responsible Role: Reporting and Analytic	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☒ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? The solution involves implementing role-based access control (RBAC) within the e-commerce report and analytics system. This separates user functionalities from system management by assigning different roles with specific permissions, restricting access to system management functions only to authorized administrators while granting users access to their designated functionalities based on their roles.	

3.13.3	Control Summary Information
Responsible Role: Payment Gateway Integration	
Implementation Status (check all that apply): ☐ Implemented ☒ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? There will be a separate account for users and admins.	

3.13.4 Prevent unauthorized and unintended information transfer via shared system resources

3.13.4	Control Summary Information
Responsible Role: Shopping Cart and Checkout	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☒ Planned ☐ Alternative implementation	

☐ Not applicable
What is the solution and how is it implemented? Solution: 1. Limit access to sensitive information and resources only to authorized personnel or systems. a. Implement Role-Based Access Control (RBAC) to ensure that individuals have access only to the information necessary for their roles. 2. Encrypt sensitive data, especially during transmission and storage, a. Using secure protocols like HTTPS to encrypt data transferred between the user's browser and the server during the shopping cart and checkout process. 3. Ensure that different user's data are properly segregated. a. Implemented by structuring databases to allocate separate sections/tables for each user's data. Database schemas are designed to isolate and categorize data, ensuring that access controls within the database prevent unauthorized access to others' information. 4. Conduct regular security audits and monitoring. a. To detect any unauthorized access attempts or anomalies in the system's behavior, regularly review and update segregation strategies to ensure they remain effective against evolving security threats and system changes.

3.13.4	Control Summary Information
Responsible Role: Payment Gateway Integration	
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? There will be different account for different system admins that will only have authority over their submodule domain	

3.13.5 Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks

3.13.15	Control Summary Information
Responsible Role: Customer Reviews and Ratings	

Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable
What is the solution and how is it implemented? To safeguard communication authenticity within the Customer Reviews and Ratings system, employ TLS encryption, strong user authentication, digital signatures, and regular updates to ensure secure and verified communication sessions.

3.13.6 Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception

3.13.16	Control Summary Information
Responsible Role: Customer Reviews and Ratings	
Implementation Status (check all that apply): ☒ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? Employ robust encryption methods, strict access controls, and conduct regular security audits to ensure confidentiality and prevent unauthorized access.	

3.13.16	Control Summary Information
Responsible Role: Recommendation Engine	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☒ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? As our engine also holds data pulled from different systems, we plan to create appropriate security measures to protect the customer's data.	

3.13.16	Control Summary Information

Responsible Role: Reporting and Analytic
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☒ Planned ☐ Alternative implementation ☐ Not applicable
What is the solution and how is it implemented? The solution involves employing robust encryption techniques for data at rest within the e-commerce report and analytics system. This encryption should utilize strong algorithms and keys to safeguard sensitive Controlled Unclassified Information (CUI) stored within the database or storage systems, preventing unauthorized access even if the data is compromised.

3.13.16	Control Summary Information
Responsible Role: Product Catalog and Inventory Management	
Implementation Status (check all that apply): ☑ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? The Product Catalog admin can ensure the products that are being stored and sold by customers will remain limit access for the tracking of each event in the inventory management.	

3.13.7 Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks

3.13.7	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☒ Not applicable	
What is the solution and how is it implemented?	

3.13.8 Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards

3.13.8	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☒ Not applicable	
What is the solution and how is it implemented?	

3.13.9 Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity

3.13.9	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☒ Not applicable	
What is the solution and how is it implemented?	

3.13.10 Establish and manage cryptographic keys for cryptography employed in organizational systems

3.13.10	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☒ Not applicable	
What is the solution and how is it implemented?	

3.13.10	Control Summary Information

3.13.11 Employ FIPS-validated cryptography when used to protect the confidentiality of CUI

3.13.11	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☒ Not applicable	
What is the solution and how is it implemented?	

3.13.12 Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device

3.13.12	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☒ Not applicable	
What is the solution and how is it implemented?	

3.13.13 Control and monitor the use of mobile code

3.13.13	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned	

3.13.13	Control Summary Information
☐ Alternative implementation ☒ Not applicable	
What is the solution and how is it implemented?	

3.13.14 Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.

3.13.14	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☒ Not applicable	
What is the solution and how is it implemented?	

3.13.15 Protect the authenticity of communications sessions

3.13.15	Control Summary Information
Responsible Role:	
IImplementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☒ Not applicable	
What is the solution and how is it implemented?	

3.13.16 Protect the confidentiality of CUI at rest

3.13.16	Control Summary Information
Responsible Role: Product Catalog and Inventory Management	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented	

3.13.16	Control Summary Information

☑ Planned
☐ Alternative implementation
☐ Not applicable

What is the solution and how is it implemented?

The Product Catalog admin can ensure the products that are being stored and sold by customer will remain limit access for the tracking of each events in the inventory management.

3.14 System and Information Integrity

3.14.1 Identify, report, and correct information and system flaws in a timely manner.

3.14.1	Control Summary Information

Responsible Role: Customer Reviews and Ratings

Implementation Status (check all that apply):
☐ Implemented
☐ Partially implemented
☒ Planned
☐ Alternative implementation
☐ Not applicable

What is the solution and how is it implemented?
establish continuous monitoring, user reporting channels, and agile response mechanisms within the Customer Reviews and Ratings system to swiftly identify, report, and correct any identified issues or system flaws.

3.14.1	Control Summary Information

Responsible Role: Recommendation Engine

Implementation Status (check all that apply):
☐ Implemented
☐ Partially implemented
☒ Planned
☐ Alternative implementation
☐ Not applicable

What is the solution and how is it implemented?
As soon the developers identify code issues, we are in response to actively handle the matter timely and swiftly.

3.14.1	Control Summary Information

Responsible Role: Reporting and Analytics

Implementation Status (check all that apply):
☐ Implemented
☐ Partially implemented
☒ Planned
☐ Alternative implementation
☐ Not applicable

What is the solution and how is it implemented?
The solution to identify, report, and correct information and system flaws in e-commerce reports and analytics involves implementing a robust data validation and error detection system. This system would continuously monitor data inputs and outputs, flagging any anomalies or errors for immediate correction, thereby ensuring the integrity and accuracy of the reporting and analytics.

3.14.1	Control Summary Information

Responsible Role: Product Catalog and Inventory

Implementation Status (check all that apply):
☑ Implemented
☐ Partially implemented
☐ Planned
☐ Alternative implementation
☐ Not applicable

What is the solution and how is it implemented?

The Product Catalog admin can ensure that the system for storing and modifying inventory will have a detailed instruction and function, and have data for tracking the events of alert.

3.14.1	Control Summary Information

Responsible Role: Payment Gateway Integration

Implementation Status (check all that apply):
☒ Implemented
☐ Partially implemented
☐ Planned
☐ Alternative implementation
☐ Not applicable

What is the solution and how is it implemented?
There will be frequent maintenance in the database

3.14.2 Provide protection from malicious code at appropriate locations within organizational systems

3.14.2	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☒ Not applicable	
What is the solution and how is it implemented?	

3.14.3 Monitor system security alerts and advisories and take appropriate actions in response

3.14.3	Control Summary Information
Responsible Role: Payment Gateway Integration	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☒ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? There will be frequents testing to ensure that notifications of vulnerabilities within the system are found	

3.14.4 Update malicious code protection mechanisms when new releases are available

3.14.4	Control Summary Information
Responsible Role: Payment Gateway Integration	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☒ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? There will be updates for 3rd party protection for viruses and external threats	

3.14.4	Control Summary Information
Responsible Role: Customer Reviews and Ratings	

Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☒ Planned ☐ Alternative implementation ☐ Not applicable
What is the solution and how is it implemented? regularly update the system from trusted sources while employing robust algorithms for data aggregation and moderation protocols to filter and authenticate information in the Customer Review and Rating system.

3.14.5 Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed.

3.14.5	Control Summary Information
Responsible Role: Payment Gateway Integration	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☒ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? There will be checking for any databases to ensure data integrity	

3.14.6 Monitor organizational systems including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks

3.14.6	Control Summary Information
Responsible Role: Payment Gateway Integration	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☒ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? There will be system failures to ensure that the proper integration incase of emergencies from external threats	

3.14.7 Identify unauthorized use of organizational systems.

3.14.7	Control Summary Information
Responsible Role: Payment Gateway Integration	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☒ Planned ☐ Alternative implementation ☐ Not applicable	
What is the solution and how is it implemented? There will be monitoring for different level of user access	