Assignment# 2

Overview of a IT Business Process & Controls

Team 8

Heiang Cheung
Nathan Van Cleave
Sarush Faruqi
James Foggie

TEMPLE UNIVERSITY

Agenda

- Review of steps taken
- Review of “storyboard” of process
- Review of identified controls
- Review of flowcharts

Steps Taken to Produce Deliverable

- Brainstormed on ideas for assignment
- Scheduled meeting to review thoughts and preliminary flows
- Fleshed out IT-Business “flow” (storyboard)
- Assigned each member to identify controls based on agreed IT-Business flow

Identified IT-Business Flow

Assumption: User is ready to purchase.

“Storyboard”

- **Open browser**, visit website

- **Prompt – Sign-In** or **New to Website** (create account)
  - Decision:
    - Existing: enter credentials
      - Enter id/Enter pwd/submit
      - Authentication
        - Pass
        - Fail
    - New Account: create account steps
      - Submit email address
      - Name
      - Submit

- **Review items in cart**
  - Confirm items for purchase
    - Decision (Cart good or changes required?)
      - Yes: Process to Checkout
      - No: Edit cart as desired

- **Proceed to Checkout**
  - **Review user order information**
    - Decision:
      - Use default shipping address?
        - Yes: Proceed
        - No: Prompt for preferred address.
          - Proceed
      - Use default payment option?
        - Yes: Proceed
        - No: Prompt for preferred payment option
      - Use default delivery option?
        - Yes: Proceed
        - No: Prompt for preferred delivery
  - **Submit Order to Amazon**
    - Decision (Edit Order?)
      - Yes: Edit order as desired
      - No: Proceed to Place Order
  - Order Confirmation
  - <Stop>

Related Controls

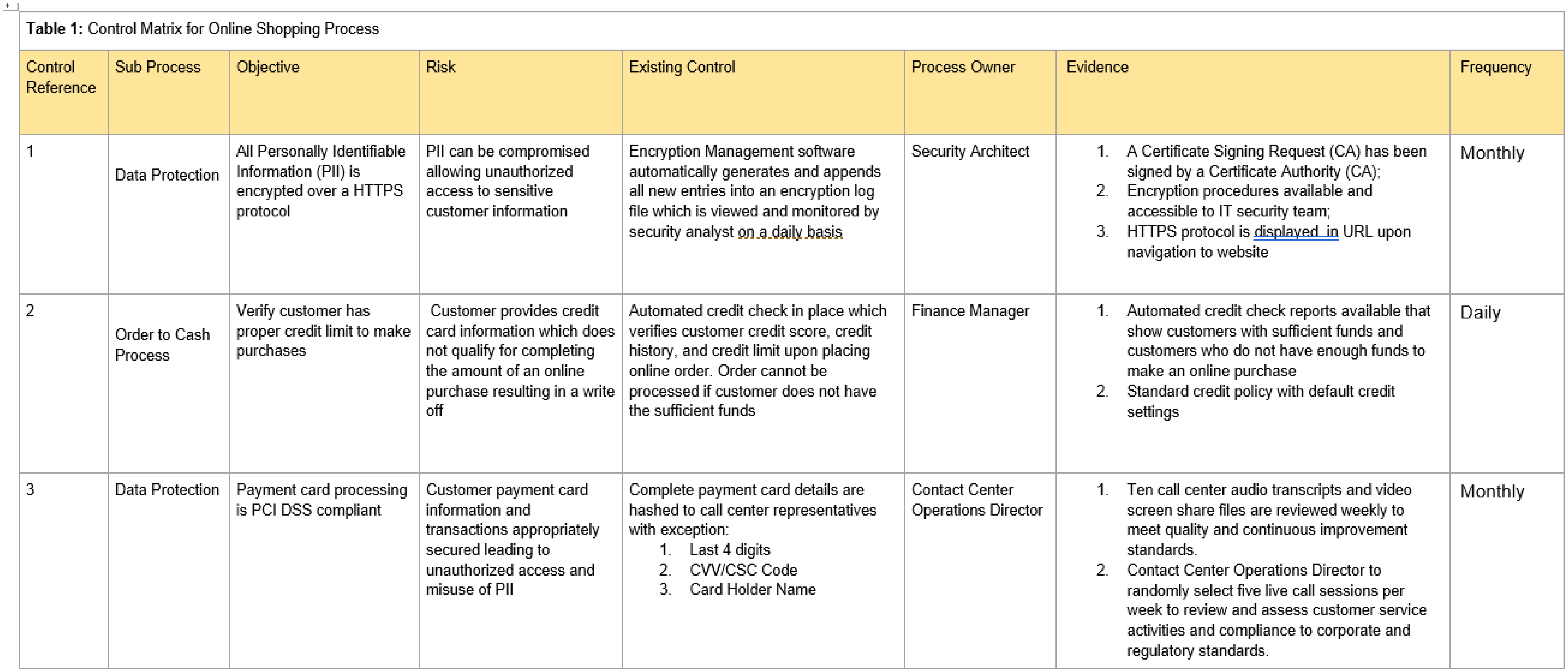


Table 1: Control Matrix for Online Shopping Process

Control Reference	Sub Process	Objective	Risk	Existing Control	Process Owner	Evidence	Frequency
1	Data Protection	All Personally Identifiable Information (PII) is encrypted over a HTTPS protocol	PII can be compromised allowing unauthorized access to sensitive customer information	Encryption Management software automatically generates and appends all new entries into an encryption log file which is viewed and monitored by security analyst on a daily basis	Security Architect	1. A Certificate Signing Request (CA) has been signed by a Certificate Authority (CA); 2. Encryption procedures available and accessible to IT security team; 3. HTTPS protocol is displayed in URL upon navigation to website	Monthly
2	Order to Cash Process	Verify customer has proper credit limit to make purchases	Customer provides credit card information which does not qualify for completing the amount of an online purchase resulting in a write off	Automated credit check in place which verifies customer credit score, credit history, and credit limit upon placing online order. Order cannot be processed if customer does not have the sufficient funds	Finance Manager	1. Automated credit check reports available that show customers with sufficient funds and customers who do not have enough funds to make an online purchase 2. Standard credit policy with default credit settings	Daily
3	Data Protection	Payment card processing is PCI DSS compliant	Customer payment card information and transactions appropriately secured leading to unauthorized access and misuse of PII	Complete payment card details are hashed to call center representatives with exception: 1. Last 4 digits 2. CVV/CSC Code 3. Card Holder Name	Contact Center Operations Director	1. Ten call center audio transcripts and video screen share files are reviewed weekly to meet quality and continuous improvement standards. 2. Contact Center Operations Director to randomly select five live call sessions per week to review and assess customer service activities and compliance to corporate and regulatory standards.	Monthly

Related Controls - continued

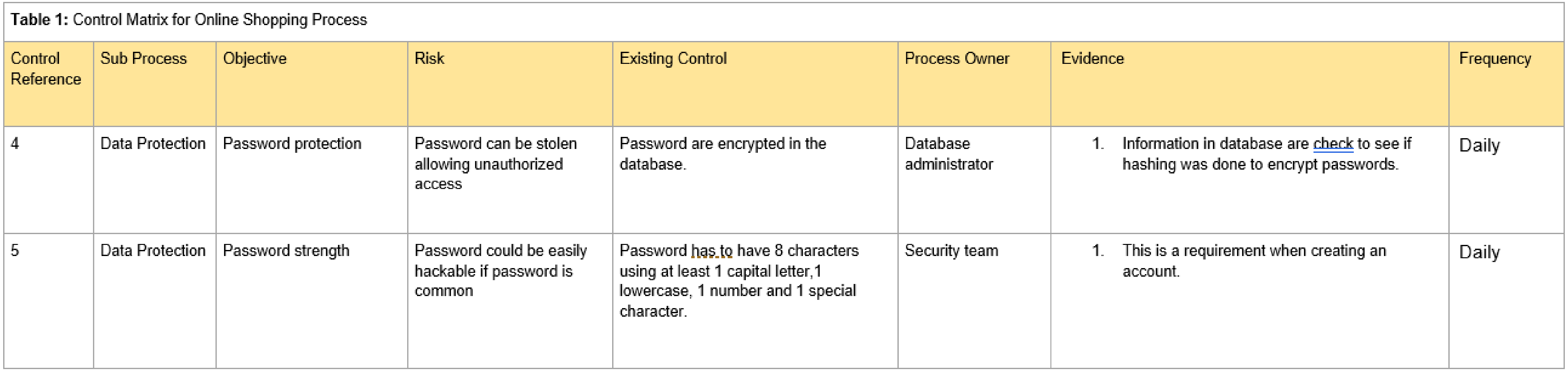
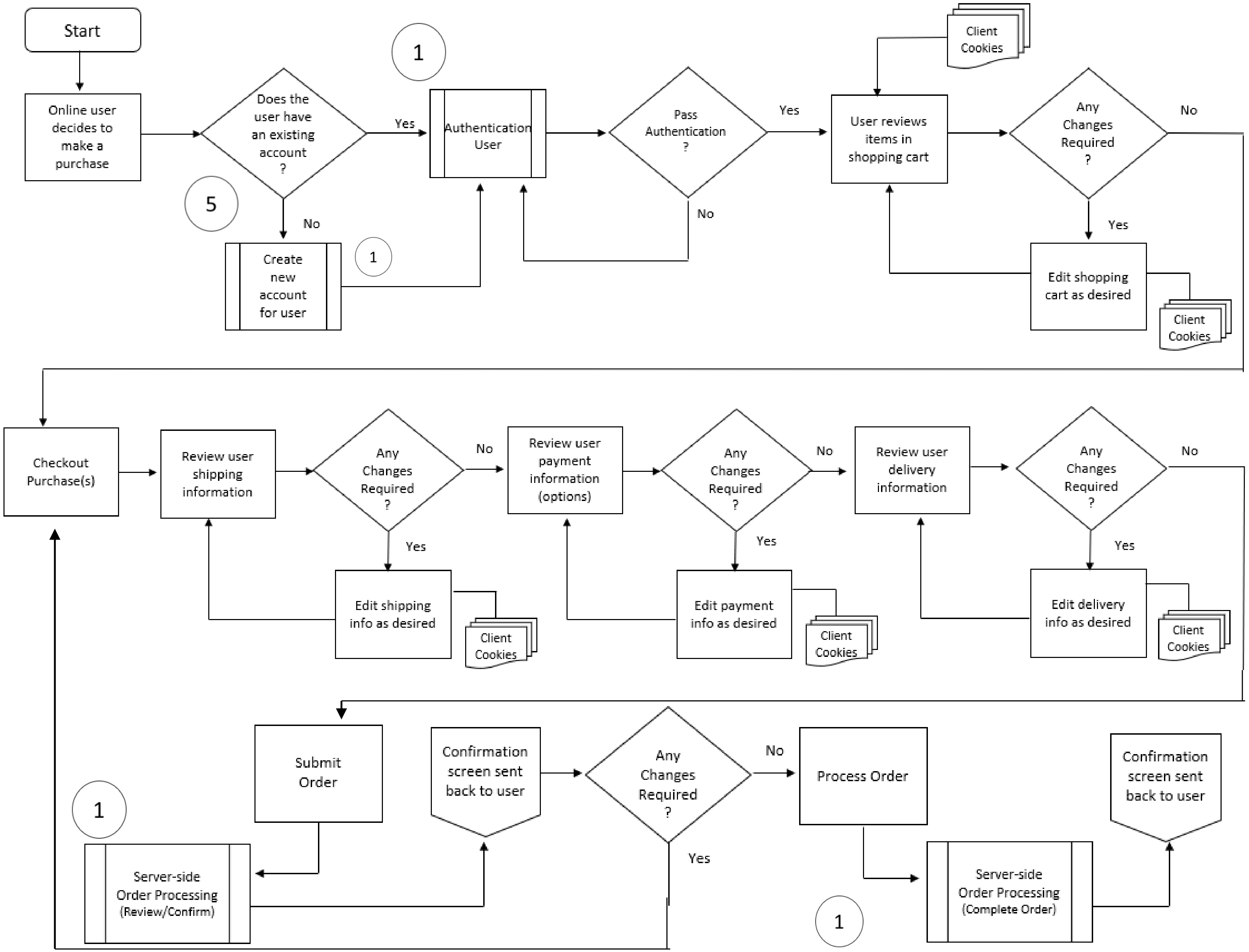


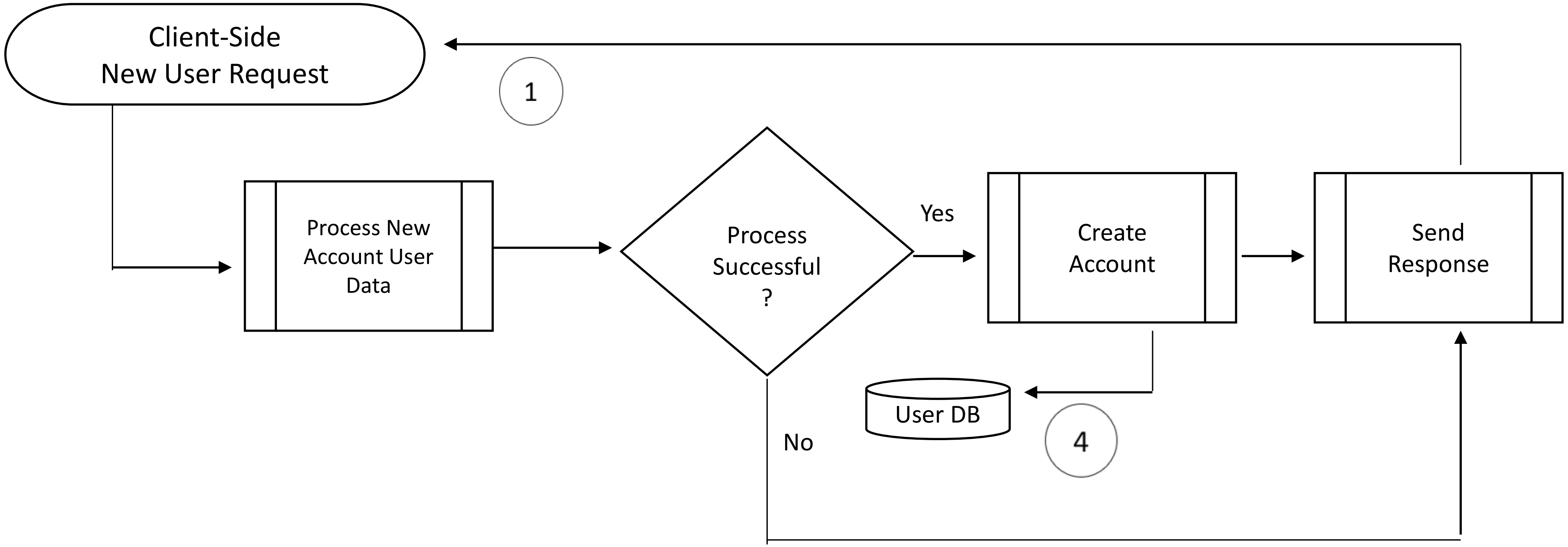
Table 1: Control Matrix for Online Shopping Process

Control Reference	Sub Process	Objective	Risk	Existing Control	Process Owner	Evidence	Frequency
4	Data Protection	Password protection	Password can be stolen allowing unauthorized access	Password are encrypted in the database.	Database administrator	1. Information in database are check to see if hashing was done to encrypt passwords.	Daily
5	Data Protection	Password strength	Password could be easily hackable if password is common	Password has to have 8 characters using at least 1 capital letter,1 lowercase, 1 number and 1 special character.	Security team	1. This is a requirement when creating an account.	Daily

Online Shopping Purchase – Process Flow **(Client-Side)**


Start
Online user decides to make a purchase
Does the user have an existing account ?
Yes
No
5
Create new account for user
1
1
Authentication User
Pass Authentication ?
Yes
No
Client Cookies
User reviews items in shopping cart
Any Changes Required ?
No
Yes
Edit shopping cart as desired
Client Cookies
Checkout Purchase(s)
Review user shipping information
Any Changes Required ?
No
Yes
Edit shipping info as desired
Client Cookies
Review user payment information (options)
Any Changes Required ?
No
Yes
Edit payment info as desired
Client Cookies
Review user delivery information
Any Changes Required ?
No
Yes
Edit delivery info as desired
Client Cookies
Submit Order
1
Server-side Order Processing (Review/Confirm)
Confirmation screen sent back to user
Any Changes Required ?
No
Yes
Process Order
1
Server-side Order Processing (Complete Order)
Confirmation screen sent back to user

Server Side: Create New Account – Process Flow



Client-Side New User Request

1

Process New Account User Data

Process Successful ?

Yes

Create Account

Send Response

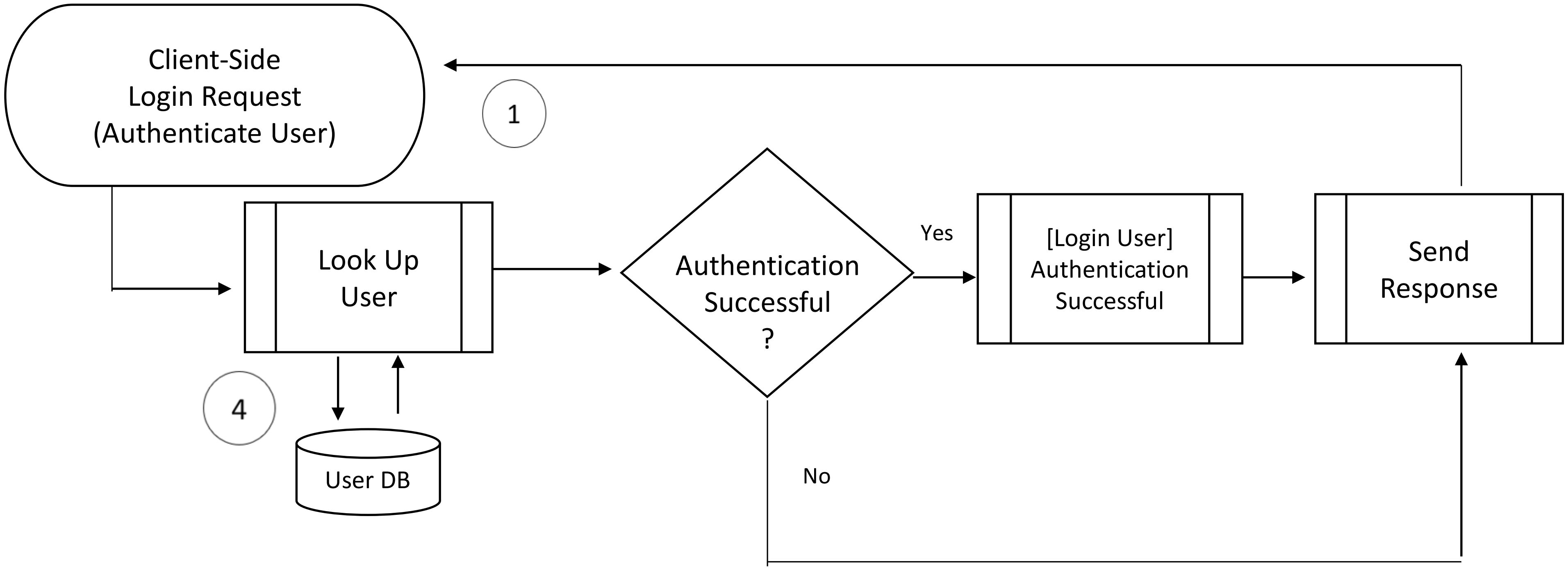
User DB

4

No

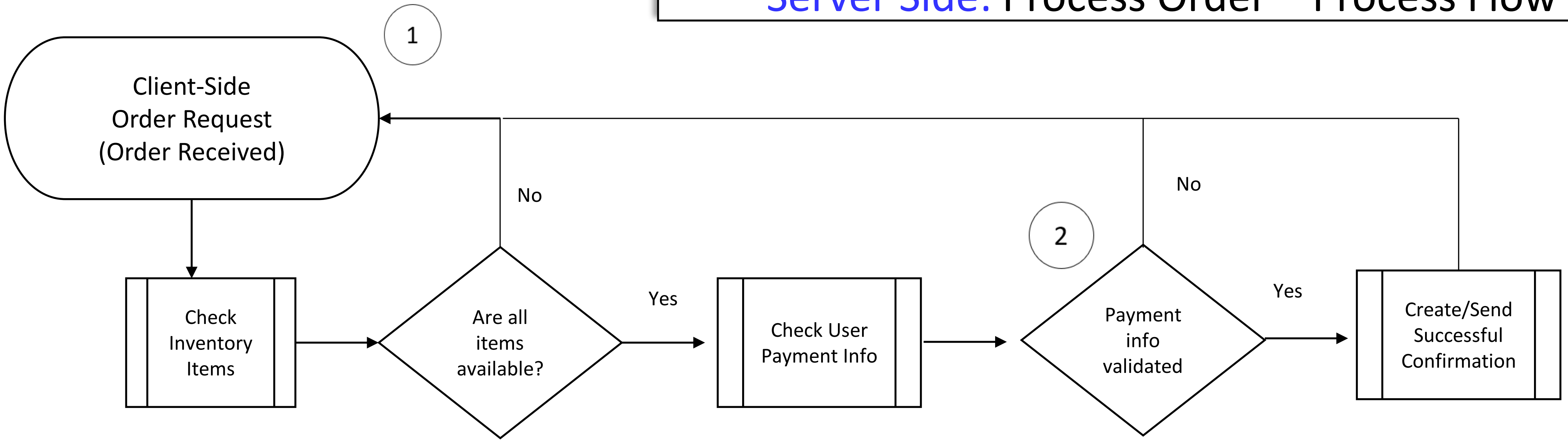
Control Reference	Sub Process	Objective	Risk	Existing Control	Process Owner	Evidence	Frequency
1	Data Protection	All Personally Identifiable Information (PII) is encrypted over a HTTPS protocol	PII can be compromised allowing unauthorized access to sensitive customer information	Encryption Management software automatically generates and appends all new entries into an encryption log file which is viewed and monitored by security analyst on a daily basis	Security Architect	1. A Certificate Signing Request (CA) has been signed by a Certificate Authority (CA); 2. Encryption procedures available and accessible to IT security team; 3. HTTPS protocol is displayed in URL upon navigation to website	Monthly
4	Data Protection	Password protection	Password can be stolen allowing unauthorized access	Password are encrypted in the database.	Database administrator	1. Information in database are check to see if hashing was done to encrypt passwords.	Daily

Server Side: User Login – Process Flow



Control Reference	Sub Process	Objective	Risk	Existing Control	Process Owner	Evidence	Frequency
1	Data Protection	All Personally Identifiable Information (PII) is encrypted over a HTTPS protocol	PII can be compromised allowing unauthorized access to sensitive customer information	Encryption Management software automatically generates and appends all new entries into an encryption log file which is viewed and monitored by security analyst on a daily basis	Security Architect	1. A Certificate Signing Request (CA) has been signed by a Certificate Authority (CA); 2. Encryption procedures available and accessible to IT security team; 3. HTTPS protocol is displayed in URL upon navigation to website	Monthly
4	Data Protection	Password protection	Password can be stolen allowing unauthorized access	Password are encrypted in the database.	Database administrator	1. Information in database are check to see if hashing was done to encrypt passwords.	Daily

Server Side: Process Order – Process Flow



1

Client-Side Order Request (Order Received)

Check Inventory Items

Are all items available?

No

Yes

Check User Payment Info

2

Payment info validated

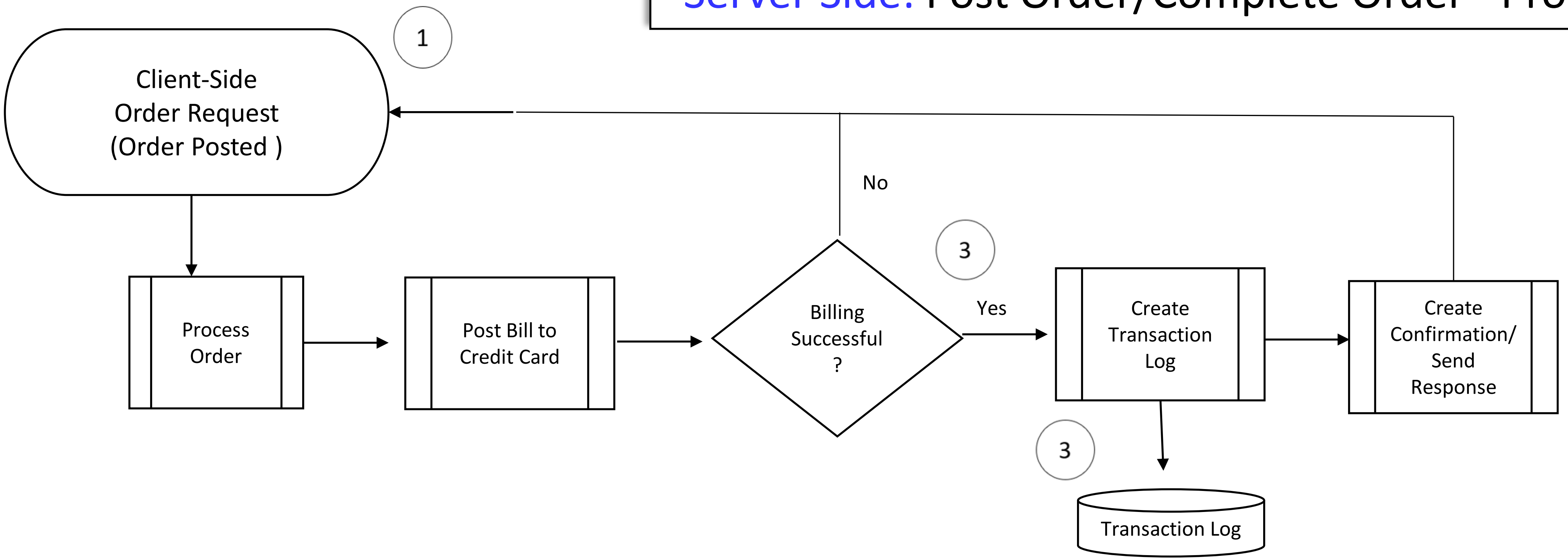
No

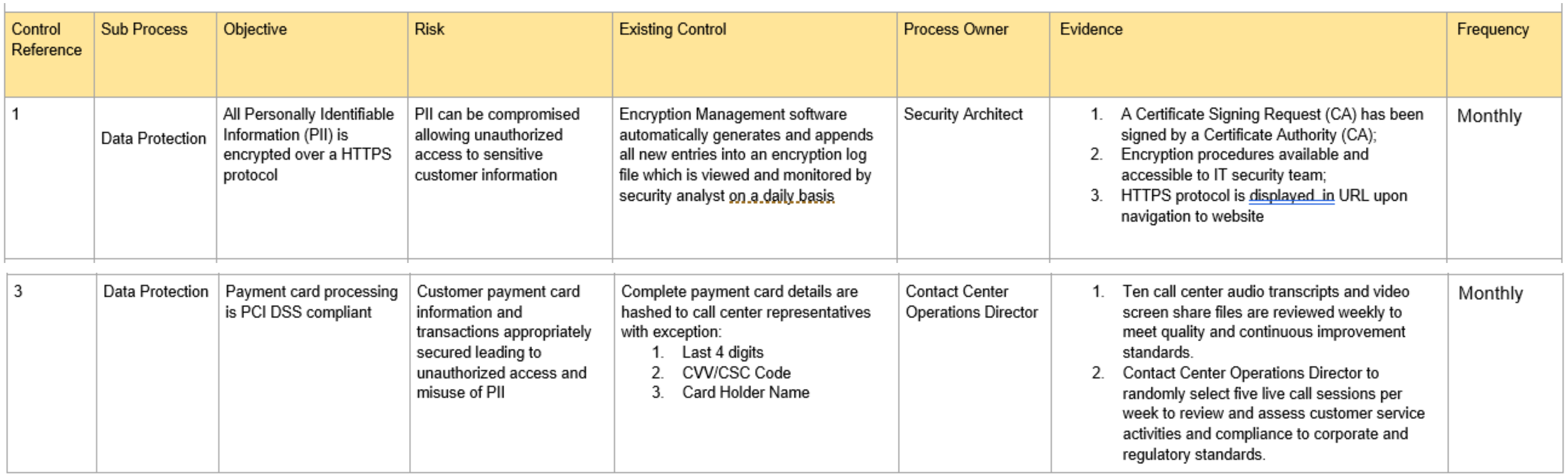
Yes

Create/Send Successful Confirmation

Control Reference	Sub Process	Objective	Risk	Existing Control	Process Owner	Evidence	Frequency
1	Data Protection	All Personally Identifiable Information (PII) is encrypted over a HTTPS protocol	PII can be compromised allowing unauthorized access to sensitive customer information	Encryption Management software automatically generates and appends all new entries into an encryption log file which is viewed and monitored by security analyst on a daily basis	Security Architect	1. A Certificate Signing Request (CA) has been signed by a Certificate Authority (CA); 2. Encryption procedures available and accessible to IT security team; 3. HTTPS protocol is displayed in URL upon navigation to website	Monthly
2	Order to Cash Process	Verify customer has proper credit limit to make purchases	Customer provides credit card information which does not qualify for completing the amount of an online purchase resulting in a write off	Automated credit check in place which verifies customer credit score, credit history, and credit limit upon placing online order. Order cannot be processed if customer does not have the sufficient funds	Finance Manager	1. Automated credit check reports available that show customers with sufficient funds and customers who do not have enough funds to make an online purchase 2. Standard credit policy with default credit settings	Daily

Server Side: Post Order/Complete Order– Process Flow





Control Reference	Sub Process	Objective	Risk	Existing Control	Process Owner	Evidence	Frequency
1	Data Protection	All Personally Identifiable Information (PII) is encrypted over a HTTPS protocol	PII can be compromised allowing unauthorized access to sensitive customer information	Encryption Management software automatically generates and appends all new entries into an encryption log file which is viewed and monitored by security analyst on a daily basis	Security Architect	1. A Certificate Signing Request (CA) has been signed by a Certificate Authority (CA); 2. Encryption procedures available and accessible to IT security team; 3. HTTPS protocol is displayed in URL upon navigation to website	Monthly
3	Data Protection	Payment card processing is PCI DSS compliant	Customer payment card information and transactions appropriately secured leading to unauthorized access and misuse of PII	Complete payment card details are hashed to call center representatives with exception: 1. Last 4 digits 2. CVV/CSC Code 3. Card Holder Name	Contact Center Operations Director	1. Ten call center audio transcripts and video screen share files are reviewed weekly to meet quality and continuous improvement standards. 2. Contact Center Operations Director to randomly select five live call sessions per week to review and assess customer service activities and compliance to corporate and regulatory standards.	Monthly

Questions
?

TEMPLE
UNIVERSITY