A Small Business Security Project

Information Security Management CRN 50252 Assessment 2 set by Dr. Lee Speakman

aslam Patel @00520874

2022

Table of Contents

[Introduction 2](#_Toc102919451)

[Design of payment system 3](#_Toc102919452)

[Preliminaries 3](#_Toc102919453)

[Flow chart of Payment operation 4](#_Toc102919454)

[How the payment will work (3D secure card payment) 5](#_Toc102919455)

[Design of Data storage Network 6](#_Toc102919456)

[Database integrated architecture 7](#_Toc102919457)

[Payment processor design 8](#_Toc102919458)

[Requirements 9](#_Toc102919459)

[Threats 10](#_Toc102919460)

[Loss of data 10](#_Toc102919461)

[Breach 10](#_Toc102919462)

[Failure of Devices/network 10](#_Toc102919463)

[Theft 10](#_Toc102919464)

[Merchant Identity fraud 10](#_Toc102919465)

[Legal consequences 10](#_Toc102919466)

[Compliance with PCI-DSS 11](#_Toc102919467)

[Installation and maintenance of firewall 11](#_Toc102919468)

[Passwords 11](#_Toc102919469)

[Card data 11](#_Toc102919470)

[Encrypt transmission of cardholder data 11](#_Toc102919471)

[Anti-virus software 11](#_Toc102919472)

[Develop and maintain Secure systems 12](#_Toc102919473)

[Restriction of card holder data 12](#_Toc102919474)

[Assign ID for employees 13](#_Toc102919475)

[Restrict physical access to cardholder data 13](#_Toc102919476)

[Track and monitor all access to network and cardholder data 13](#_Toc102919477)

[Regular testing 13](#_Toc102919478)

[Maintenance of policy in relation to security for employees. 14](#_Toc102919479)

[CIS Critical Security Controls 15](#_Toc102919480)

[01 Inventory and Control of Enterprise Assets 15](#_Toc102919481)

[02 Inventory and Control of Software Assets 15](#_Toc102919482)

[03 Data Protection 15](#_Toc102919483)

[04 Secure Configuration of Enterprise Assets and Software 15](#_Toc102919484)

[05 Account Management 15](#_Toc102919485)

[06 Access Control Management 15](#_Toc102919486)

[07 Continuous Vulnerability Management 15](#_Toc102919487)

[08 Audit Log Management 16](#_Toc102919488)

[09 Email and Web Browser Protections 16](#_Toc102919489)

[10 Malware Defences 16](#_Toc102919490)

[11 Data Recovery 16](#_Toc102919491)

[12 Network Infrastructure Management 16](#_Toc102919492)

[14 Security Awareness and Skills Training 16](#_Toc102919493)

[15 Service provider management 16](#_Toc102919494)

[17 Incident response management 16](#_Toc102919495)

[Compliance with GDPR 17](#_Toc102919496)

[Conclusions and recommendations 18](#_Toc102919497)

*The total word count excluding references, figure captions, introduction and table of contents is* ***3256****.*

# Introduction

*This paper is attempts to find a solution to Good Farm Shops (GFS) to supply them with an integrated electronic payment system for the 3 shops they own. The main benefit of using integrated payment systems is that it saves time.*

*Alongside this all payments will be logged against each members membership account which will be stored on databases.*

*There will be an additional database which will be implemented to allow for the stock of all three shops being managed, to allow for the database to automatically alter the stock levels when purchases a made.*

# Design of payment system

## Preliminaries

**Customer:** A customer is a person who purchases goods and pays for them on time.

**Merchants:** A merchant is a seller who will receive payments made by customers in this case Good Farm Shops (GFS).

**Client bank:** The client bank is in charge of the customers bank account and verifies the consumer payment.

**Merchant bank:** Merchant bank accounts are held by Merchant bank. It is in charge of management, fraud prevention, and so forth.

**Payment Gateway:** Used for interconnectivity between all users connected to the process. The internet is a key tool for this and it is responsible for reliability and security of transactions between all users.

This shows the multiple streams of data and connections that the payment authorisation will have to deal with, in reality it is showing the preliminary factors that will be needed for GFS.

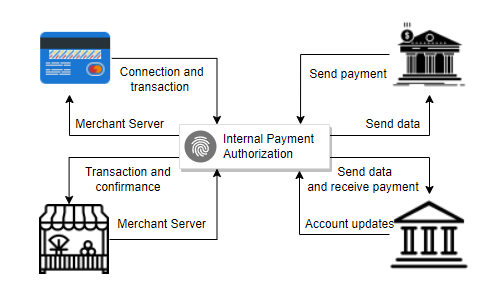


Figure Payment flow

## Complete design

Diagram

Description automatically generated

Figure 2 Full system Design

Branch 2 will hold the main database server which will be connected to the branch 1 and branch 3 sub databases which will only hold inventory data not customer data. Only the main database will hold customer membership data.

## Flow chart of Payment operation

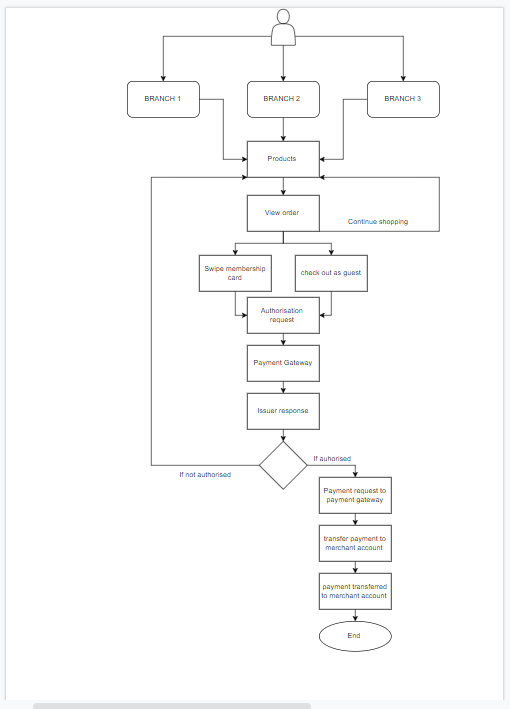


Figure Flow chart of full operation

## How the payment will work (3D secure card payment)

For the card payment there will be a POS system where the details of the customers will be captured which will be on the sellers’ side. Diagram

Description automatically generated

Figure 3D payment using SSL

Once the card is inserted the details will be entered over SSL which will be sent to the GFS application.

Again, over the SSL this will be sent to the payment gateway which will then be in xml json format but the gateway will convert this to ISO 8583 which is now the standard for these types of payments.

It will then be sent to the payment processor now the payment processor is used by merchants acquiring bank in most cases payment gateway and payment processor will be used together

Thereafter they will redirect the request to the issuer bank for example, Lloyds who will authorise the payment for the customer.

## Design of Data storage Network

Diagram

Description automatically generated

Figure Database only Network design

## Database integrated architecture

Diagram

Description automatically generated with medium confidence

Figure Database integrated architecture

The payment ingest system is used in each branch and save the transaction by using a transaction ID generator to track each transaction. This will be stored in the Main database.

The main database will hold the transaction ID (type of payment) and items bought (barcodes) and add it to the member ID number if membership is used and provide a discount for users for those purchases if membership is found.

Because GFS will be getting so many queries every second we will partition all your table of data based on date so every day will have one partition. We can also create a sub partition for RDBMS so that sub partition can be based on the type of the transaction and many more factors.

The messages will be stored in the distributed queue which will be picked up by the payment processor and ultimately update each sub database.

## Payment processor design

Diagram

Description automatically generated

Figure Payment processor design

The Payment processing service once the payment is done it will update the status of the payment in the database and in case of failure it will put the message in a failed queue. This is key as the payment retry service will work with this queue to attempt to retry failed payments.

Since the transaction id is unique when it makes a request to the card issuer bank based on the same transaction ID it will receive a status with payment already processed, therefore not duplicating the payment.

The clearing service is used to read the database and it will pick up all the successful transaction and add it to the main database if it is successful or not. The main purpose of clearing process is to pick up all the transactions that are not cleared yet.

## Requirements

We will ensure the following requirements for GFS.

**Functional requirements**

* Allow multiple ways of payments e.g., visa, Mastercard, apple pay, gift cards, membership balance etc.
* Secure payments
* Secure transactions (no failure from merchant side
* Avoid double payment
* Fast response
* Handle time out and failure (if timed out)

**Non-functional requirements**

* Consistent
* Highly available
* Scalable if more branches are being considered in the future.

# Threats

## Loss of data

When a cybercriminal effectively penetrates datasets and obtains sensitive material, this is known as a data breach. This can be accomplished physically by gaining physical access to a computer or network in order to take local files, or virtually by circumventing network security. The latter is frequently used to target businesses. *(Segal, 2022)*

If data is corrupted or lost as a result of a breach, it can have a significant negative impact on GFS. GFS's vital data, such as membership IDs, purchase history, and subscriptions, can be lost, requiring the databases to be refilled.

## Breach

If the payment system designed within this solution is hacked by a cybercriminal then a lot of private customer information can be gathered, including, card details, names and addresses, email addresses which can be used to gain capital from GFS’ customer base.

Not only that the merchant banking details can potentially be extracted for the use of fraud if not immediately then in the future. *(Bush, 2022)*

If a SQL injection attack is successfully completed then the database which holds this customer data will be compromised. *(Bush, 2022)*

A simple reconnaissance can also be completed by a potential rival without stealing capital rather only by stealing customer habits. *(Ommani, 2022)*

## Failure of Devices/network

A failure of any end devices will result in a negative impact for GFS. Customers will expect visit a branch and pay using an alternative way but will be declined.

## Theft

If any end devices such as a PDQ machine is physically stolen the fraudster can potentially set up reverse/refund payments to an account of their choice resulting to a breach of GFS’ bank details. *(Ommani, 2022)*

## Merchant Identity fraud

If an attacker gets their hands on GFS credentials using the payment network, they can open a merchant account in the name of GFS company and charge stolen credit cards resulting in a false identity fraud. *(Segal, 2022)*

## Legal consequences

When GFS payment system connects its network to the Internet, it becomes vulnerable to cyber-attacks.

GFS could be held negligent if we acquire information from clients and that information is hacked by cybercriminals. Data breaches caused by outside hackers are a major issue for GFS.

# Compliance with PCI-DSS

PCI-DSS applies to all retailers and service providers who process, transmit, or store cardholder data.

## *Installation and maintenance of firewall*

The first line of defence for GFS network is a firewall. The firewall chosen is a cisco ASA firewall.

This will cover the entire network across the 3 branches including each POS system and PDQ machine.

This approach adds numerous checkpoints to the network firewall's security, necessitating full endpoint protection.

## P*asswords*

This focuses on protecting GFS systems such as, *network devices, databases, and firewalls*.

The factory default settings for usernames, passwords, and other unsafe setup options are included in most operating systems and devices.

All passwords will be generated from a random password generator (containing 12 characters with a mixture of letters numbers and symbols) and stored in the reputable password storage application.

Not only passwords, configurations, code, SQL etc will be stored in a similar manner, *alongside updates every time a new system in added to the infrastructure.*

## *Card data*

To protect GFS customers stored card data we feel this is the most important factor. We have decided to only store the following data:

* Payment Type
* Card type
* Transaction ID
* Loyalty member information

The transaction ID will hold the bulk of the information regarding the data for example, cost, issuer bank, merchant bank etc.

This ID will be encrypted with the AES-256 algorithm and will aid GFS to secure customer data.

We will use the CDD software to scan for all unencrypted data across all file systems to ensure that we can pinpoint data such as PAN, CVV, PIN etc which will be scanned on a weekly basis.

## *Encrypt transmission of cardholder data*

This is similar process to the above requirement.

Majority of the card data will be processed by the payment gateway and the processor so as the payment system will be using SSL this should ensure that the data will not get compromised, *again the usage of CDD will aid in detecting any unencrypted data within the public domain.*

## *Anti-virus software*

The Anti-virus software that will be used will be the Kaspersky small office security which will allow GFS to install and in essence forget about it.

ESNnS will remotely manage and update the anti-virus for the 3 branches.

## *Develop and maintain Secure systems*

Implementing security upgrades as soon as possible is critical to GFS’ security posture. All important components in the card flow pathway will be patched, including:

* Browsers (internet browsers)
* Firewalls
* Databases for application software
* POS machines
* System software
* PDQ machines
* PC’s

This will be completed in accordance with the requirements of “one month into release” and monitored at the end of each week.

## *Restriction of card holder data*

This requirement is all about role-based access control (RBAC), which allows only those who need to know access to card data and systems.

Only specific individuals will have access to certain data with specific levels of privilege. Proposed access levels shown below:

|  |  |  |
| --- | --- | --- |
| **Job title** | **Access** | **Privilege level** |
| **Branch 1, 2, 3 management** | - Customer ID  - Transaction ID  - Customer Name  - Issuer Bank  - Failed Payments | **Medium** |
| **Branch 1, 2, 3 Employees** | - Customer ID  - Transaction ID  - Customer Name | **Low** |
| **Regional Manager** | - Customer ID  - Transaction ID  - Customer Name  - Issuer Bank  - Tax documents  - Bank documents  - Failed Payment details | **High** |
| **ESNnS** | - Customer ID  - Transaction ID  - Customer Name  - Issuer Bank  - Tax documents  - Bank documents  - Failed Payment details  -Database access  - payment resource access | **High** |

## *Assign ID for employees*

We will not be using any shared or group credentials. A unique identifier will be assigned to each authorised user, and passwords must be sufficiently complex. All passwords will be generated randomly and kept in a reliable password storage application.

To track all transactions and payments, all customers will be issued an optional Membership ID and a 6-digit pin.

A two-factor authentication will also be in place for all PC’s, cash registers and PDQ machines to restrict any unauthorized access and monitoring employees by documenting times, actions etc.

## *Restrict physical access to cardholder data*

This requirement is concerned with the security of physical access to systems containing cardholder information. Unauthorized individuals could obtain access to the installation and steal, disable, interrupt, or destroy important systems and cardholder data if physical access restrictions are not in place.

We will install a mesh network within each branch, which will use video surveillance to keep track of physical locations like access and exit doors, cashier.

## *Track and monitor all access to network and cardholder data*

We will document the following:

* Who has access to protected environments, and why do they require it?
* Which applications are available on each and every device
* What components are used at specific times, the reasons for use and where they are used in the shop.

## *Regular testing*

We will ensure all security updates and patches have been installed but they will also be tested. This will be to detect any vulnerabilities within our design that will be accessible for attackers.

We will carry out three main tests:

* Vulnerability scan: A high level scan which will detect and report vulnerabilities within the payment design network. This will be carried out quarterly by scanning all IP’s and all domains
* Penetration Testing: this will be used to exhaust the system with a series of tests to exploit any weakness within our system.
* Fraud analytic tests: used to monitor income of revenue and the source of revenue.

## *Maintenance of policy in relation to security for employees.*

The final PCI compliance criterion is to maintain paperwork, policies, procedures, and proof relevant to GFS’ security measures.

The following will be included:

* Employee roles and manuals
* Company polices and procedures
* Any third-party vendors
* All incident response plans.

# CIS Critical Security Controls

Reference to the controls can help ESNnS with both CSI-DSS compliance and GDPR.

## *01 Inventory and Control of Enterprise Assets*

**1.1:** with the aid of GFS, a member of ESNnS will identify any unauthorized assets 2 times a week. An employee may no longer need access therefore they will be removed. This will be to respond to security threats for devices.

## *02 Inventory and Control of Software Assets*

**2.3:** ESNnS will continually monitor if any software is removed from any of the end devices by employees accidentally or intentionally. In addition to this any software which has been added to either network or to any of the end devices. We will respond to this by either adding the software back or deleting the software and making management of GFS aware of this.

**2.4:** ESNnS will be sure to support all software installed on PC’s, PDQ’s and other end devices. All software will have its relevant documentation and protocols for its use. We will review all software’s used once a month.

## *03 Data Protection*

**3.3:** ESNnS will ensure that all employees of ESNnS and GFS have been given a unique ID with varied permissions for each user for local, database, and network systems. This is to ensure the protection of client and merchant data for GFS.

## *04 Secure Configuration of Enterprise Assets and Software*

**4.3:** We will configure for all End-devices and sessions opened by all users of GFS to last a total of 15 minutes when not in use. This will be implemented on all branches of GFS for the POS, PDQ and PC. If there is a separate session opened on the PC by the employee to check for customer data then this will be limited to 2 minutes. This will be implemented for the protection of the network and data.

## *05 Account Management*

**5.3:** ESNnS will disable all accounts with no activity within a timeframe of 30 days. This will be implemented to respond to employees.

**5.2:** A random password generator will be used for created of employee accounts to protect the employees accounts.

## *06 Access Control Management*

**6.1:** Any sort of access within the network of GFS will need to be authorised prior. If a new role is required for one employee they will need to get this authorised for access, this is to protect the users.

## *07 Continuous Vulnerability Management*

**7.1:** A high level scan which will detect and report vulnerabilities within the payment design network. This will be carried out quarterly by scanning all IP’s and all domains. This will be done to protect all applications and devices on the network.

## *08 Audit Log Management*

**8.2:** The three branches will produce an audit log each month. ESNnS will collect all of the logs on a monthly basis to monitor the performance of the network. This will be used to detect any inconsistencies within the network or potential suspicious activity.

## *09 Email and Web Browser Protections*

**9.1:** We will only use the browser Mozilla Firefox across all end devices of GFS. A company domain will also be set up under the name of @GFS.Grocery.com to allow for secure email for all employees of GFS, with only management allowed further access. This is to protect GFS.

## *10 Malware Defences*

**10.2:** Our Kaspersky antivirus will update to its newest version automatically with authorisation from ESNnS.

## *11 Data Recovery*

**11.2:** We will back up all data onto another database, which will hold the exact same information of records, customers etc. this will be carried out automatically every 24 Hours. This is to recover any data that might get corrupted.

## *12 Network Infrastructure Management*

**12.2:** ESNnS will review weekly for any hardware/software updates which may be needed for additional effectiveness for GFS. Ultimately to protect the network from Attacks.

## *14 Security Awareness and Skills Training*

**14.3:** ESNnS will hold a training week for all employees across all three branches to inform on the current social engineering attacks that are in work. The main focus will be on phishing. This is to protect the business security as whole.

## *15 Service provider management*

**15.1:** ESNnS will work with GFS to create a list of service providers to ensure we know is dealing with GFS. The inventory of service providers will be updated each month to identify new aspects to the business.

## *17 Incident response management*

**17.2:** 1 member of the ESNnS will be available for response on any suspicious activity either spotted by ESNnS or GFS on a designated secure telephone line which will be available 24 hours a day. Policy will be to find source of attack or which device on network breached and respond with relevant action from the SOP(which system/server to close down).

# Compliance with GDPR

The proposed solution ESNnS has provided will be compliant with GDPR to ensure that there is no room for non-compliance resulting in any failure in brand damage.

We aim to collect the following personal data from our membership customers:

* Customer Name
* Customer address
* Customer Number
* Customer email address
* Branch 1/2/3
* Payment reference

The above 6 data sets will be used for and is necessary for the performance of a contract. As GFS are offering a membership service to customers GFS it brings the *“legal obligation to provide that service”* and these main 6 data sets are required also to *“protect the vital interests of customers”*.

Non membership customers will have the following data collected:

* Branch 1/2/3
* Payment reference

For the following reasons “compliance with a legal obligation” ,“*protect vital interest”* and *“performance of contract”.*

All payment receipts, transaction codes, times etc. will be kept on the database payment storage system for an indefinite period. This is due to the main reasons:

* *“Statistical purposes”*. Where GFS will aim to gather trends across a given time period of their choice
* Also, as GFS will be classed as the *“Data controller”* they will be responsible for this data for the purpose of dealing with refunds, overpayment etc. *(GDPR protection law 2022)*

# Conclusions and recommendations

The proposed design aims to solve the cash only problem GFS have. By using design elements alongside with compliance with CIS, PCI-DSS and GDPR for the solution GFS can aim to increase their customer base, customer tracking and maybe even customer marketing and targeted advertisement .

The main advantage for GFS is that it will allow them to minimize mistakes, lessen time and analyse critical data collected by the membership, stock, and customer database.

With the rise of the *“lazy age”* we would further recommend GFS to consider implementing an online ordering and payment system in which customers can order on a GFS website and collect instore using their unique collection code.

We also suggest they consider a move to cloud-based system to keep all data and networks centralised, this will assist them to manage data more efficiently.

# References

*Bush, T., 2022. SWOT Analysis Threats: Definition & Examples. [online] PESTLE Analysis. Available at: <https://pestleanalysis.com/swot-analysis-threats-definition-examples/> [Accessed 2 April 2022].*

*European Commission - European Commission. 2022. Who does the data protection law apply to?. [online] Available at: <https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/application-regulation/who-does-data-protection-law-apply\_en> [Accessed 3 April 2022].*

*Ommani, A., 2022. Strengths, weaknesses, opportunities and threats (SWOT) analysis for farming system businesses management:. [ebook] Department of Agricultural Management, Shoushtar Branch, Islamic Azad University, p.Varied Pages. Available at: <https://academicjournals.org/article/article1380639652\_Ommani.pdf> [Accessed 1 May 2022].*

*Pcisecuritystandards.org. 2022. Official PCI Security Standards Council Site - Verify PCI Compliance, Download Data Security and Credit Card Security Standards. [online] Available at: <https://www.pcisecuritystandards.org/pci\_security/maintaining\_payment\_security> [Accessed 01 May 2022].*

*Lecture slides from Information security management Module | Dr. Lee Speakman | University of Salford | Accessed throughout*

*Segal, E., 2022. The 10 Biggest Risks and Threats For Businesses In 2022. [online] Forbes. Available at: <https://www.forbes.com/sites/edwardsegal/2022/01/05/the-10-biggest-risks-and-threats-for-businesses-in-2022/> [Accessed 24 April 2022].*