90%

Information Security Management – 2025

Information Security Within An Organisation

Information Security Project Report

Table of Contents

Introduction

British Farm Shops (BFS) have contracted our team at Salfordo Networks n' Stuff (SNnS) to provide a secure network solution for stock tracking, smart payment and membership cards. This report starts with the proposed network architecture and security measures against the main threats. This is followed by an evaluation of the solution's compliance with PCI-DSS, CIS Critical Security Controls, and the UK GDPR to ensure that this solution follows both the industry standard frameworks and legal grounds in the UK.

Section 1. Design Outline

1.1 Network Architecture Diagrams

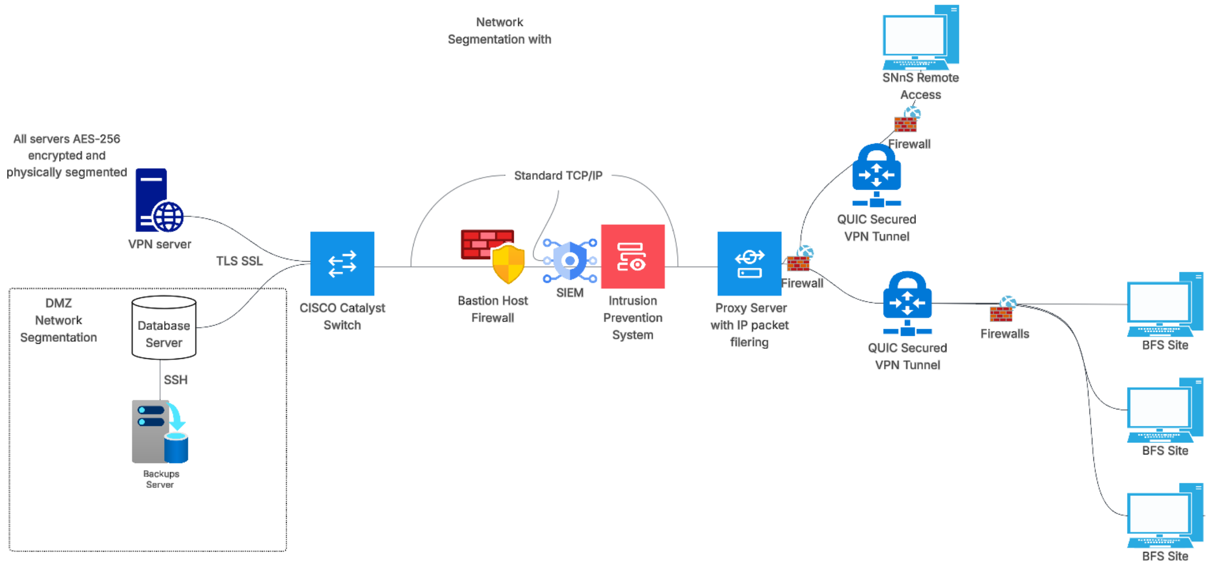


Figure 1: Overall Network Architecture

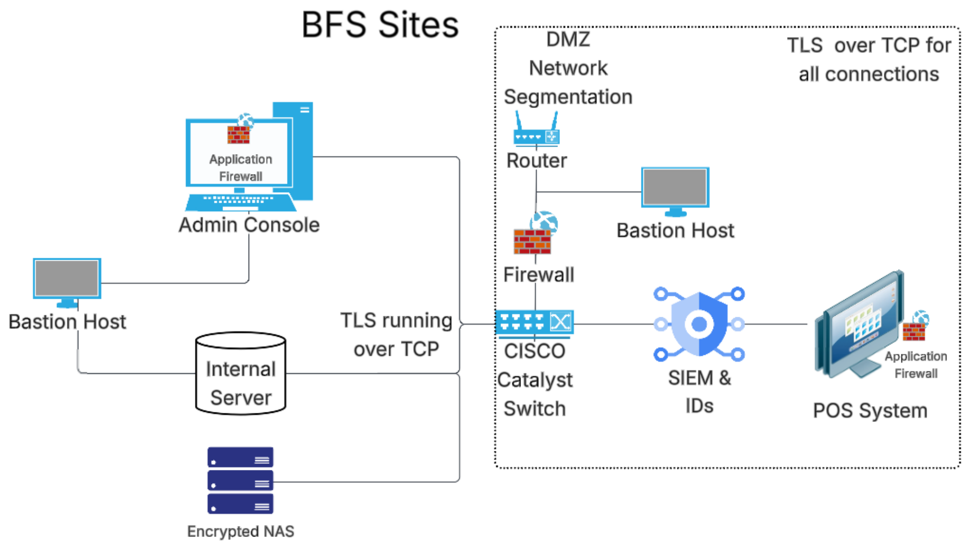


Figure 2: BFS Site/Shop Network Architecture

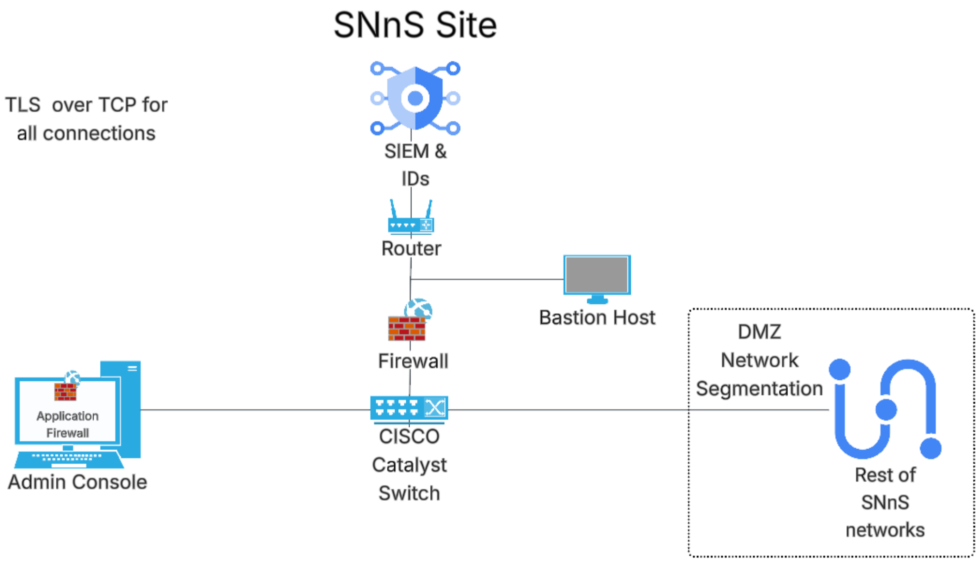
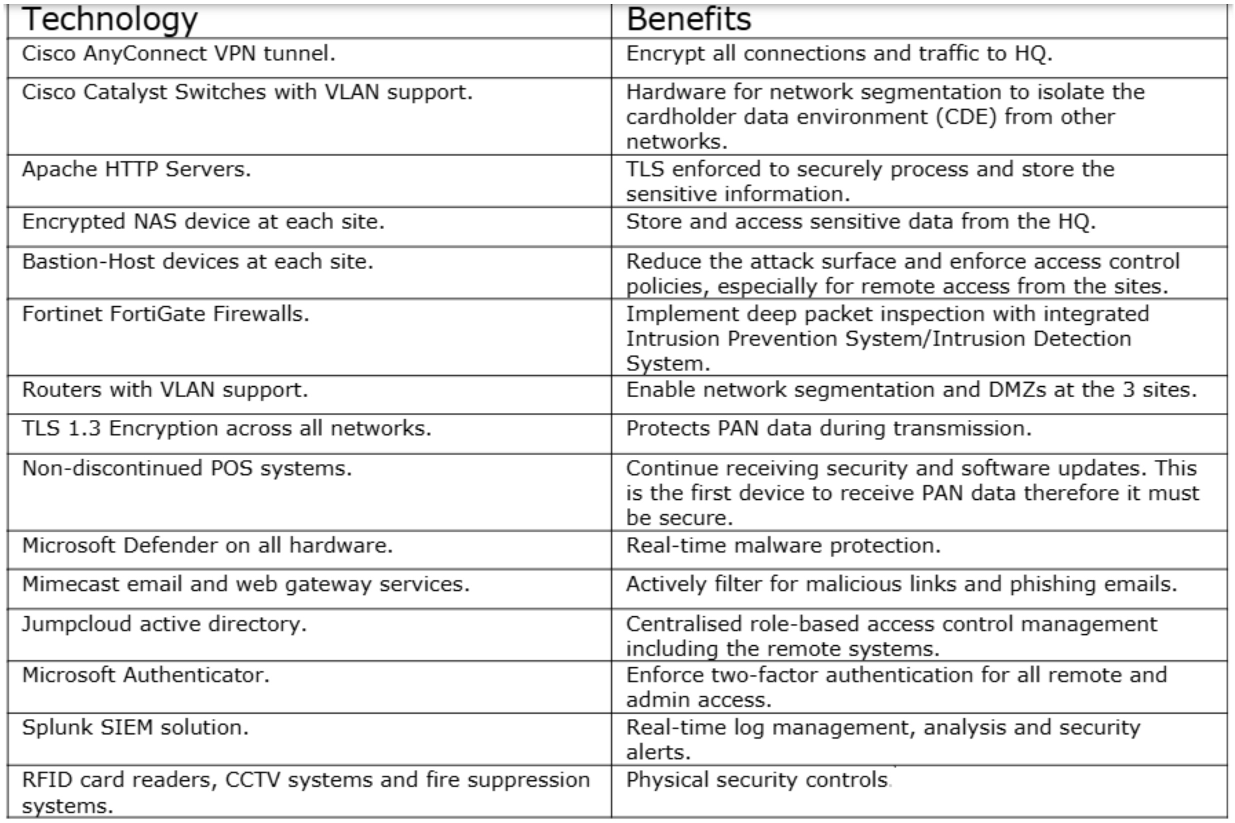


Figure 3: SNnS Site Network Architecture

1.2 List of Technologies

As demonstrated in the network architecture diagram, QUIC protocol built on UDP is the communication protocol that will be used as part of the VPN tunnel to transmit data between the 3 sites, SNnS and the HQ. QUIC (Quick UDP Internet Connections) is a new encrypted-by-default Internet transport protocol, that provides a number of improvements designed to accelerate HTTP traffic compared to TCP as well as make it more secure. (Ghedini, 2018) The protocol between the Cisco Catalyst Switch and the VPN and Database servers is TLS (Transport Layer Security) which encrypts the data, running on top of TCP (Transmission Control Protocol).

This networking solution is an intranet with controlled external access via secure VPNs and DMZs. Considerations were made to refine this list of technologies to better suit BFS's objectives and organisation size. This included balancing cost-effective solutions with strong security features, ensuring scalability for the company's future growth, and selecting secure, yet accessible solutions for remote access.



Technology	Benefits
Cisco AnyConnect VPN tunnel.	Encrypt all connections and traffic to HQ.
Cisco Catalyst Switches with VLAN support.	Hardware for network segmentation to isolate the cardholder data environment (CDE) from other networks.
Apache HTTP Servers.	TLS enforced to securely process and store the sensitive information.
Encrypted NAS device at each site.	Store and access sensitive data from the HQ.
Bastion-Host devices at each site.	Reduce the attack surface and enforce access control policies, especially for remote access from the sites.
Fortinet FortiGate Firewalls.	Implement deep packet inspection with integrated Intrusion Prevention System/Intrusion Detection System.
Routers with VLAN support.	Enable network segmentation and DMZs at the 3 sites.
TLS 1.3 Encryption across all networks.	Protects PAN data during transmission.
Non-discontinued POS systems.	Continue receiving security and software updates. This is the first device to receive PAN data therefore it must be secure.
Microsoft Defender on all hardware.	Real-time malware protection.
Mimecast email and web gateway services.	Actively filter for malicious links and phishing emails.
Jumpcloud active directory.	Centralised role-based access control management including the remote systems.
Microsoft Authenticator.	Enforce two-factor authentication for all remote and admin access.
Splunk SIEM solution.	Real-time log management, analysis and security alerts.
RFID card readers, CCTV systems and fire suppression systems.	Physical security controls

Table 1: List and detail of the technologies that have been chosen.

Section 2. Threat Analysis

The proposed network architecture in section 1 is designed for secure remote administration and data processing. This section identifies the significant threats that have been identified and assesses the countermeasures in place to mitigate these threats.

2.1 Threats within the organisation

Dissatisfied agents operating within the organization are the main source of cybercrime. (Li and Liu, 2021) BFS employees who have the authority to access the HQ database could download a malicious application or misuse their authority for their own gain. This could include data exfiltration of all the sensitive business data, or misusing company hardware or system resources for cryptocurrency mining. The main cause of accidental insider data breaches is poor employee education around security and data protection and can be avoided by practicing good security practices. (Tekleselase Woldemichael, 2020)

As BFS have not employed their own technical staff, their staff may be untrained on cyber risks in the workplace, and this increases the risk of misconfiguring the systems in place and exposing the network to threats contained on their personal devices.

Applying role-based access controls helps to mitigate these threats. PCI-DSS requirement 7 has been implemented to ensure principle of least privilege is also enforced. PCI-DSS requirement 5 as well as CIS Control 14 have been implemented which include training and educating employees which will help to mitigate this threat.

2.2 Distributed Denial of Service (DDoS) Attack

Distributed Denial of Service attacks are the main categories of attacks that can affect availability at the network level. (De Donno et al., 2019) This would greatly disrupt the operations at BFS starting with the POS and payment systems failing to communicate with the HQ, disrupting all sales. The stocks tracking system will also be disrupted, leading to irregular entries and possibly a recount of all items which would be costly for the company.

This threat is mitigated by the security controls in section 4. Compliance with CIS Control 13 (Network Monitoring and Defence) includes the use of a firewall with DDoS mitigation features to block suspicious traffic. The proposed network will also perform traffic filtering between network segments at each store to prevent any malicious attackers from gaining access to other parts of the network. (CIS, 2024)

2.3 Remote Access Exploitation

This solution allows for SNnS to perform remote administration from the company's site. If this is not properly secured this will be an attack vector for attackers to exploit the authentication protocols and gain unauthorised access to the BFS HQ and their shops. This could lead a disruption of service or data exfiltration of the sensitive business and customer data; Remote data integrity checking protocols are required for this purpose. (De Donno et al., 2019)

This threat is mitigated by implementing PCI-DSS requirement 8, enforcing multi-factor authentication at all BFS sites and at SNnS, along with all remote connections requiring an authenticated VPN connection with Transport Layer Security (TLS). As mentioned in section 3.8, remote desktop protocol (RDP) is in place to only allow authorised access to the HQ from key management staff.

2.4 Compromised POS Systems

The BFS shops have POS systems to allow customers to purchase goods and scan their membership cards. As these systems are visible to all customers in their shops, these systems are a common target for attacks. Attackers can tamper these devices or inject malware to compromise the sensitive business and personal data such as stocks tracking data and customer cardholder information. The payment processors can be targeted to allow attackers to bypass payments, leading to unauthorised sales of goods.

This threat is mitigated by implementing CIS Controls safeguard 12.2, isolating the POS systems in a DMZ via network segmentation. All transactions are encrypted and monitored with logs stored on servers at each BFS site. Implementing CIS Controls safeguard 2.2 and 7.3 ensures these systems have regular software updates from the manufacturer to ensure the latest security patches are in place. Controls safeguard 7.5 is implemented with continuous security monitoring (CSM) with an on-premises Security Information and Event Management (SIEM) tool, which also ensures that threats are handled proactively. (PurpleSec, 2024)

2.5 Insecure transmission and storage

Sensitive information including cardholder and membership data is transmitted between the shop and BFS HQ, or the internet where necessary for payment processing. This information is at risk both during transmission and when stored on the servers at each shop and HQ. This can be intercepted or breached by attackers if kept without encryption, compromising the confidentiality and integrity of the data.

This is mitigated by enforcing TLS 1.3, the latest the latest version of the Transport Layer Security protocol during data transmission. TLS 1.3 requires the encrypted TLS handshake for a secure connection and has removed the less secure cryptographic ciphers from previous versions, ensuring a secure transfer of data. AES-256 encryption is used on the servers as well as the backups at the HQ, which uses a 256-bit key to encrypt and decrypt data. (Progress Software, 2022) This ensures compliance with GDPR as described in section 5, as the sensitive information is impenetrable to all brute-force attacks.

Section 3. Compliance with PCI-DSS

PCI-DSS has 12 core requirements for critical security controls. This section outlines how the proposed solution in section 1 aligns with these requirements, assessing the safeguards within the payment systems and the overall network architecture.

In this section, all text in italics are references to the PCI-DSS Quick Reference Guide - PCI, 2025.

3.1. *Requirement 1: Install and Maintain Network Security Controls*

Technical requirements

Implement Network Security Controls (NSCs) such as firewalls or virtual network security processes.

Network access must include restrictions to and from the cardholder data environment (CDE).

Non-technical requirements

Document the policies and procedures for the firewall rules.

The processes for installing and maintaining NSCs such as network architecture diagrams must be defined and understood.

Compliance

Requirement 1 has been met with firewalls in place at each shop and the HQ to enforce segmentation between the cardholder data environment and the external networks. TLS-secured VPN tunnels are in place to secure all communication between each site and the HQ and as shown in section 1, network architecture diagrams are in place. Each site also has SIEM systems to passively monitor all network traffic and flag anomalies to alert the technicians at SNnS to any suspicious activity.

3.2. *Requirement 2: Apply secure configurations to all system components*

Technical requirements

Default accounts for all devices and software must be replaced and default passwords must be changed.

Unnecessary services must be removed, and all systems and wireless services should be configured and managed securely.

Non-technical requirements

The procedures and methods in place to apply secure configurations across all system components are clearly outlined and understood.

Compliance

Requirement 2 has been met with the default user credentials and passwords being updated on all systems and hardware. The wireless access points at each shop will be secured with WPA3 and MAC filtering and contained in a DMZ, segmented from the admin console which is used to access the main database at HQ.

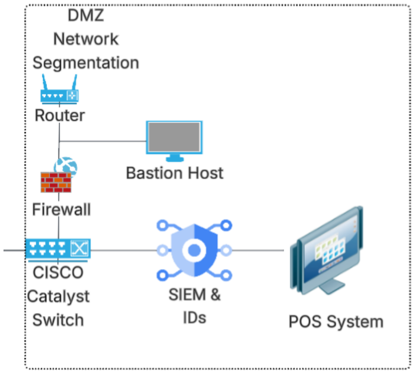


Figure 4: Network segmentation at BFS stores.

3.3. *Requirement 3: Protect Account Data*

Technical requirements

PAN data is stored securely with encryption with cryptographic keys at rest and only kept for as long as necessary.

Only authorised personnel can access PAN data.

Security controls are implemented to ensure unauthored access does not occur.

Non-technical requirements

A data retention policy is in place to minimise the storage of sensitive data.

Procedures in place for data protection are documented and reviewed when necessary.

Compliance

Only the HQ database contains the limited storage of PAN at rest, which is encrypted using AES-256 with cryptographic keys and only accessible to authorised personnel.
Cryptographic keys will be managed through a centralized key management system that enforces strong key generation and secure storage with access control procedures. These keys will be regularly rotated and securely destroyed. *Payment account data* will *not be stored unless it is necessary to meet the needs of the business.* (PCI, 2025) All payment account data will only be stored for as long as needed, including for those customers with membership cards which is also compliant with the GDPR in section 5.

3.4. *Requirement 4: Protect cardholder data with strong cryptography during transmission over open, public networks*

Technical requirements

The processes for protecting cardholder data during transmission is documented.

All transmissions of PAN and cardholder data must use strong cryptography.

Compliance

Requirement 4 has been met as all data in transit from the 3 shops is securely transmitted via QUIC Secured VPN Tunnels. PAN data is not transmitted over public networks.

3.5. *Requirement 5: Protect all systems and networks from malicious software*

Technical requirements

Anti-malware software is installed and regularly updated on all devices and anti-malware processes are in place.

Email and web-content filtering are in place to defend against phishing attacks.

Non-technical requirements

Malware protection policies and countermeasures are documented and understood.

User training procedures are in place.

Compliance

Anti-malware mechanisms are in place at all sites via the firewalls, with anti-malware software within each admin console and server. Real-time scanning and logging via an on-premises Security Information and Event Management (SIEM) passively monitors for threats as mentioned in section 2.4. SNnS will deliver security awareness training to all staff at BFS, raising awareness of the threat vectors such as social engineering, phishing attacks, using weak passwords and downloading malicious software. Anti-phishing filters will be in place at all email systems used by employees to help mitigate these threats.

3.6. *Requirement 6: Develop and maintain secure systems and software*

Technical requirements

Regularly patch all systems to apply security updates.

Secure coding practices are in place for all custom software and countermeasures against the OWASP top 10 threats are in place on all company websites.

Static analysis should be performed on events flagged as suspicious by the SIEM software.

Non-technical requirements

Maintain documentation of all assets and software lifecycle for all custom software.

Compliance

Requirement 6 has been met with the implementation of SIEM software for regular vulnerability scanning as described in section 3.5. All POS systems will get regular software updates with security and software patches from the manufacturers. All custom software will follow the software development lifecycle, following secure coding practices.

3.7. *Requirement 7: Restrict access to cardholder data by business need-to-know*

Technical requirements

Enforce role-base access control with procedures in place to restrict access to sensitive information. Implement the principle of least privilege across all systems.

Non-technical requirements

Document the access control policies and procedures in place to safeguard cardholder data and ensure that these policies are understood.

Compliance

Role-based access controls are in place with the principle of least privilege on all systems and devices. Access to the database at HQ is restricted to authorised personnel, and other employees are restricted to a strict scope of systems within the DMZ. Implementation of requirement 10 includes logs at each site as well as at the HQ to be kept and reviewed regularly.

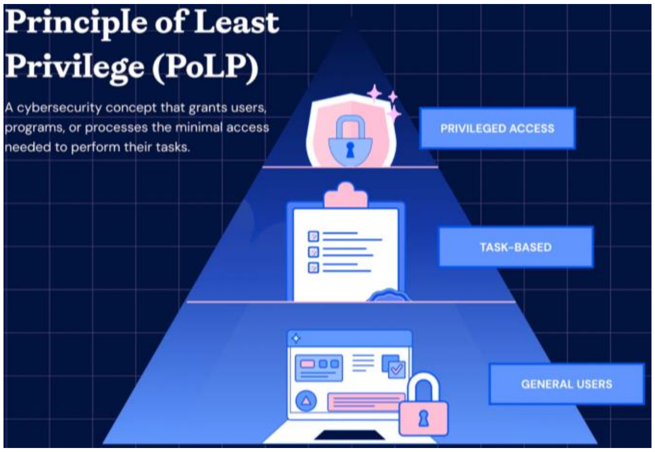

Principle of Least Privilege (PoLP)
A cybersecurity concept that grants users, programs, or processes the minimal access needed to perform their tasks.
PRIVILEGED ACCESS
TASK-BASED
GENERAL USERS

Figure 5: The PoLP triangle. (Wiz Experts Team, 2024)

3.8. *Requirement 8: Identify users and authenticate access to system components*

Technical requirement

Implement and strictly manage the account policies for both users and admins with strong password requirements and multi-factor authentication (MFA).

Compliance

MFA is enforced on all POS systems and the admin consoles for remote access via the VPNs. Remote access protocol in place at SNnS to allow a remote connection to the HQ and includes filters to restrict connections to authorised computers with limited access times. Each user has unique credentials, and each system logs all activity which is then monitored. Account policies include deprovisioning, promptly revoking access to ex-employees and suspicious accounts. (Sanjay Maljure, 2024) Passwords are regularly updated for all accounts, with strict password requirements.

3.9. *Requirement 9: Restrict physical access to cardholder data*

Technical requirements

Facilities storing cardholder data must be secured using access badges, and CCTV cameras.

Non-technical requirements

The servers and backup storage devices must have physical security measures in place. Visitor logs and access control policies are understood. Staff are trained on physical security controls.

Compliance

Staff are trained by SNnS to recognise and respond to threats as mentioned in sections 3.5 and 2.1. All sites all have restricted, access-controlled server and admin console rooms. Surveillance systems are in place, and all devices are inspected to detect tampering.

3.10. *Requirement 10: Log and monitor all access to system components and cardholder data*

Technical requirements

Record all access to systems and cardholder data with time-synchronisation. Review logs to identify failures in the critical security controls and securely store the logging history.

Non-technical requirement

The procedures for taking logs, accessing and reviewing logs are defined and understood.

Compliance

Logging is in place at all sites, including access to all restricted systems such as admin consoles, as well as firewalls and POS devices with backups stored at the HQ. As mentioned in section 3.5, SIEM software regularly conducts vulnerability scanning which includes these logs to review all activity and report to SNnS when failures in the critical security controls are identified.

3.11. *Requirement 11: Test security of systems and networks regularly*

Technical Requirements

Monitor for network intrusions and unauthorised access, devices or access points. Regularly vulnerability scans and penetration tests, including external testing.

Compliance

Internal and external penetration testing will be regularly performed on the remote access systems as well as the cardholder data environment within the POS systems in the DMZ. As mentioned in section 3.5, SIEM software is in place to regularly conduct vulnerability scanning.

3.12. *Requirement 12: Support information security with organizational policies and programs*

Non-technical requirements

Documentation of the security incident response systems and acceptable use policy. Staff training and risk assessments.

Compliance

A cyber incidence response plan will be in place with documentation of how to prepare for and respond to a breach. Staff will be trained as mentioned in section 2.1 and third-party service providers (TPSPs) will be investigated to assess whether their services follow our PCI-DSS policy.

Section 4. CIS Critical Security Controls

This section outlines how the solution implements IG1 Safeguards from these 18 CIS Critical Security Controls to provide basic cyber hygiene against the most common attacks. Implementation Group (IG) 1 safeguards are for small to medium-sized enterprises with limited IT and cybersecurity expertise to dedicate towards protecting IT assets and personnel. (CIS, 2024)

In this section, all text in italics are references to the CIS Critical Security Controls® Version 8.1. (June 2024).

Control 01: Inventory and Control of Enterprise Assets

Safeguard 1.1 Establish and Maintain Detailed Enterprise Asset Inventory.

We will keep an inventory of all *enterprise assets with the potential to store or process data.* This information will be kept in the secure database server at HQ and will include metadata like IP, OS version, hardware specs, verified, and owner.

Safeguard 1.2 Address Unauthorized Assets.

Automated network scans will take place once a week to log all assets and identify unauthorised devices. Further action on unauthorised devices will be up to the discretion of the team at SNnS based on the risk to the organisation and can include employee training as described in control 14.

Control 02: Inventory and Control of Software Assets

Safeguard 2.2 Ensure Authorized Software is Currently Supported.

All software used at BFS will be documented and include monthly reviews for security updates and depreciation dates. No depreciated software will be used, and all software will be updated promptly.

Control 03: Data Protection

Safeguard 3.3 Configure Data Access Control Lists.

As mentioned in section 3.7; the principle of least privilege and role-based access controls will be in place*, applied to all file systems, databases, and applications.*

Safeguard 3.4 Enforce Data Retention.

Data will be retained according to BFS's data retention policy. As mentioned in section 5.3, PII data is only retained for as long as necessary.

Control 04: Secure Configuration of Enterprise Assets and Software

Safeguard 4.4 Implement and Manage a Firewall on Servers.

All sites will include firewalls with separate firewalls at the HQ for the database and backup servers.

Safeguard 4.7 Manage Default Accounts on Enterprise Assets and Software.

As described in section 3.2; default user credentials and passwords will be updated on all systems and hardware.

Control 05: Account Management

Safeguard 5.2 Use Unique Passwords.
Every device/service will require users to use unique passwords as a strong password policy will be enforced. Employee training provided by SNnS will help to educate employees on cybersecurity practices.

Safeguard 5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts.

As mentioned in section 3.7; the principle of least privilege and role-based access controls will be in place. Administrative or ‘root’ privileges will only be given to the *dedicated administrator accounts* controlled by SNnS.

Control 06: Access Control Management

Safeguard 6.1 Establish an Access Granting Process.

Role-based access controls will enable access to be granted automatically to users who gain higher security clearance.

Safeguard 6.3 Require MFA for Externally-Exposed Applications.

All *externally-exposed enterprise or third-party applications* will force MFA using Microsoft authenticator.

Control 07: Continuous Vulnerability Management

***Safeguard 7.4 Perform Automated Application Patch Management**.*
Applications will be automatically updated with all security or feature updates from the manufacturer(s).

Control 08: Audit Log Management

Safeguard 8.3 Ensure Adequate Audit Log Storage.
Logs are stored in the internal servers at each site, then transmitted using

TLS to the backup server at the HQ. Mentioned in section 2.5; AES-256 encryption is used on the servers as well as the backups at the HQ.

Control 09: Email and Web Browser Protections

Safeguard 9.1 Ensure Use of Only Fully Supported Browsers and Email Clients.

Only fully supported web browsers and email clients will be used at all sites, with automated security and feature updates on all devices.

Safeguard 9.2 Use DNS Filtering Services.
Dns filtering blocklist will be in place to block access to and from known malicious sources. Cloudflare Gateway will also be in place.

Control 10: Malware Defenses

Safeguard 10.1 Deploy and Maintain Anti-Malware Software*.*
SNnS will ensure anti-malware software is installed in all enterprise assets. Windows firewall and Microsoft Defender on computers and end-devices, CrowdStrike Falcon within the Servers and automated network traffic analysers on all routers and switches.

Control 11: Data Recovery

Safeguard 11.2 Perform Automated Backups.

Automated backups of all enterprise assets will take place monthly.

Safeguard 11.3 Protect Recovery Data
The backups mentioned in 11.2 are stored securely in the encrypted backup server at HQ. Data separation is also in place to protect all types of data.

Control 12: Network Infrastructure Management

Safeguard 12.1 Ensure Network Infrastructure is Up-to-Date.
As mentioned in Control 9.1, automated security and feature updates are in place on all devices. There will be monthly reviews for security updates and depreciation dates as mentioned in Control 2.2.

Control 14: Security Awareness and Skills Training

14.1 Establish and Maintain a Security Awareness Program.

14.2 Train Workforce Members to Recognize Social Engineering Attacks.

***14.5 Train Workforce Members on Causes of Unintentional Data Exposure**.*

14.6 Train Workforce Members on Recognizing and Reporting Security Incidents

SNnS will deliver security awareness training to all staff at BFS, raising awareness of the threat vectors such as social engineering, phishing attacks, using weak passwords and downloading malicious software, as mentioned in section 2.4. This will also include recognising and reporting security incidents and an awareness programme educating employees about the different causes for unintentional data exposure.

Control 15: Service Provider Management

15.1 Establish and Maintain an Inventory of Service Providers.

An inventory of all service providers and their contact details will be established, maintained and classified in regards to the cyber risks associated with each service. This inventory will be reviewed and maintained annually, *or when significant enterprise changes occur that could impact this Safeguard.*

Control 17: Incident Response Management

17.1 Designate Personnel to Manage Incident Handling.

The team at SNnS will manage incident handling, with one member at BFS overseeing our operations.

17.2 Establish and Maintain Contact Information for Reporting Security Incidents.

SNnS and BFS will both maintain a list of all parties, verified annually, in case of a security incident, including key SNnS security engineers, security staff at BFS, *law enforcement, cyber insurance providers, relevant government agencies, Information Sharing and Analysis Center (ISAC) partners, or other stakeholders.*

Section 5. Compliance with the Data Protection Act – GDPR

In the UK, data protection is governed by the UK General Data Protection Regulation (GDPR) and the Data Protection Act 2018. (Gov.uk, n.d.) The UK GDPR sets out seven key principles which lie at the heart of the general data protection regime. (ICO, 2023) This section outlines how the proposed solution is currently and will be in compliance with the UK GDPR and DPA 2018.

Personally Identifiable Information (PII) and other personal data that may be used or retained by BFS includes Cardholder name, Primary Account Number (PAN), Billing address, Phone number, Email address, IP address and other identifiers.

In this section, all text in italics are references to the UK GDPR and Data Protection Act 2018- Gov.uk, 2018.

5.1. *The information is used fairly, lawfully and transparently. (Gov.uk, n.d.)*

The processing and retention of all personal data has a lawful basis and will be carried out with consent from customers. The information will be used transparently with documentation of how and why the PII was used and how the processing may affect the customers. Storage limitation policies will be in place for the different types of data BFS stores and reviewed regularly to ensure personal data is erased or anonymised when it is no longer needed. The lawful basis for contracts will apply for all data relating to membership services as BFS will need to process customer's personal data to comply with the obligations under the contract. (ICO, 2023)

5.2. The information is used for specified, explicit purposes (Gov.uk, n.d.)

The processing and retention of personal data will be documented and periodically reviewed. This is focused on tracking all purchases, customer memberships, and facilitating payment by debit/credit/membership card and related smart payment. All usage and storage of the personal information mentioned above will be for this purpose only and communicated to customers when they sign up for memberships. Customers will have the right to rectify and the right to erasure.

5.3. The information is used in a way that is adequate, relevant and limited to only what is necessary (Gov.uk, n.d.)

Only data that is necessary for the functions mentioned in section 5.2 will be collected, rather than a broad range data that could include unnecessary personal data. All personal data will be periodically reviewed to ensure the information is adequate and relevant. The amount of information held will differ for the different types of personal data that is stored e.g. PAN data will have different limitations to membership cardholder data, which will include the customer's email and home address. This focus on data minimisation complies with principle 3.

5.4. The information is accurate and, where necessary, kept up to date (Gov.uk, n.d.)

All banking and PAN data will be sent to the issuing banks for validation before a transaction is made through the POS systems, per industry standards. All inaccurate records of personal data will be erased or rectified without delay as advised by the Information Commissioner's Office. (ICO, 2023) BFS will also store all records of purchases including cancellations, refunds and adjustments to show all the changes that were made and ensure accuracy in the records.

5.5. The information is kept for no longer than is necessary (Gov.uk, n.d.)

PII will be kept for as long as the membership is active and may exceed this time period for administration purposes or other relevant and adequate reasons in compliance with principle 3. This time period will be communicated to the customers when they sign up for a membership. A standardised retention policy will be in place as a guideline for how long to retain all types of personal data.

5.6. The information is handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage (Gov.uk, n.d.)

Article 32 of the UK GDPR includes encryption as an example of an appropriate technical measure. (ICO, 2023) As mentioned in section 3.3, only the database at the HQ contains the limited storage of PAN, which is encrypted using AES-256 and only accessible to authorised personnel. Key authorised staff will be educated on encryption, and there will be an encryption policy in place outlining how and why the data is encrypted. Personal information will be transmitted through secure communication with TLS.

5.7. Accountability

This principle outlines the organisation’s willingness towards compliance with the GDPR throughout their future operations. BFS should understand the GDPR and assess their practices of the 6 principles above with a comprehensive privacy management programme including reports, audits and privacy awareness throughout the organisation. (ICO, 2023)

Section 6. Conclusions and Recommendations

Conclusions

The proposed solution has met all of the requirements set by British Farm Shops with technology solutions that guarantee the confidentiality, integrity and availability of data at all times. The design outline is compliant with PCI-DSS and CIS-CSC and this report includes all the changes to the infrastructure and the organisation that are needed to ensure compliance with the industry standards when the systems and networks are built.

Recommendations

When implementing this solution, it is important that both BFS and SNnS ensure security is given the highest priority for all design decisions. Compliance with PCI-DSS includes roadmaps and regular reviews of the systems in place; this is a good reference point for continuously maintaining the systems in the future. There should be a focus on integrating the current secure systems in use at BFS sites e.g. POS systems while ensuring that any new technologies implemented can be centrally monitored and scale as BFS expands.

References

All quoted headings, control names and phrases in italics are references to the standards reviewed in each section. For example, section 3 reviews PCI-DSS, and the text in italics are references to the PCI DSS Quick Reference Guide.

Ghedini, A. The Cloudflare Blog. The Road to QUIC. (July 2018)
https://blog.cloudflare.com/the-road-to-quic/

Li, Y. and Liu, Q. A comprehensive review study of cyber-attacks and cyber security; emerging trends and recent developments. (November 2021)

https://doi.org/10.1016/j.egyr.2021.08.126

De Donno, M., Giaretta, A., Dragoni, N., Bucchiarone, A. and Mazzara, M. Cyber-Storms Come from Clouds: Security of Cloud Computing in the IoT Era. Future Internet. (June 2019)

https://doi.org/10.3390/fi11060127

Tekleselase Woldemichael, H. Emerging Cyber Security Threats in Organization. International Journal of Information and Communication Sciences. (April 2020)

https://doi.org/10.11648/j.ijics.20200502.12

Center for Internet Security (CIS), CIS Critical Security Controls® Version 8.1. (June 2024)

https://learn.cisecurity.org/cis-controls-v8-1-guide-pdf

Victor Kananda, Progress Software, Why You Should Use AES 256 Encryption to Secure Your Data. (June 2022)

https://www.progress.com/blogs/use-aes-256-encryption-secure-data

Joshua Selvidge, Jason Firch, PurpleSec. Why Continuous Security Monitoring Is A Requirement In 2024. (September 2024)

https://purplesec.us/learn/continuous-security-monitoring/

PCI Security Standards Council PCI DSS Quick Reference Guide. (January 2025)

https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Supporting%20Document/PCI-DSS-v4_x-QRG.pdf

Sanjay Maljure, CloudView Partners, User Provisioning and Deprovisioning: A Guide for IT Teams (September 2024)

https://cloudviewpartners.com/user-provisioning-and-deprovisioning/

Information Commissioner's Office. *A Guide to the Data Protection Principles*. Information Commissioner’s Office. (n.d, 2023)
https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles

UK Government. Data Protection Act. Gov.uk. (n.d., 2018)
https://www.gov.uk/data-protection

Wiz Experts Team, wiz.io. What is the principle of least privilege (October 2024)
https://www.wiz.io/academy/principle-of-least-privilege-polp