FRONT SHEET
Individual Coursework

CANDIDATE NUMBER (C-NUMBER)	C2086715
MODULE NAME	Data Security
WORD COUNT	2400
SUBMISSION DATE	06.02.2024

DECLARATION

I certify that this assessment submission is entirely my work and I have fully referenced and correctly cited the work of others, where required. I also confirm the contents of my submission have not been generated by a third party or through an Artificial Intelligence generative system*.

I have read the Student Discipline Regulations (Student Discipline Regulations) and understand any Assessment Related Offence/ Academic Misconduct may result penalties being applied.

By submitting this assessment submission, I am confirming that I am fit to sit according to the Assessment Regulations.

I declare that:

- This is my own unaided work.
  Yes ☒
  No ☐

- The word count stated by me is correct.
  Yes ☒
  No ☐

- I'm happy for my work to be retained on the Elite repository and made available to staff and future students
  Yes ☒
  No ☐

*Please note that all the assignments are submitted to Turnitin.
Please note personal information (such as names) will be deleted.

Instructions to candidates:

1. Please complete this cover sheet by entering your Candidate Number, Module Name, Word Count, and Submission Date.
2. You must NOT use your NAME on this cover sheet or on any part of your coursework.

Table of Contents

Executive Summary

This assessment report closely evaluates the essential elements of data security, focusing on the digital architecture of a system for booking hotels online and a system for selling things in stores (POS).

In the context of the online hotel booking system, the report highlights the importance of robust password validation, demonstrating this with Python code examples. It further delves into the criticality of encryption and decryption methods in safeguarding user data and emphasizes the necessity of multifactor authentication (MFA) for enhanced security.

For POS systems, the assessment extensively discusses the implementation of the ISO 27001 framework, underscoring its significance in bolstering information security management. Additionally, the PCI DSS framework's role in protecting cardholder data is elaborated upon, providing insights into compliance strategies and real-world applications. The report concludes by emphasizing the paramount importance of data security across these platforms and recommends **on-going** updates and monitoring of security measures to combat evolving cyber threats. It also advocates for stringent policy implementation and suggests an exploration into emerging data security technologies and the adaptation of security policies in response to new threats and regulatory changes.

Important Terminology

In order to reflect the wider applicability of information resources of any size or complexity, organised specifically for the collection, processing, use, sharing, dissemination, maintenance, or disposition of data or information, the term "system" is used for this report in place of the term "information system."

Other important terms to know are:

- AI**:** Artificial Intelligence means the use or study of computers or tools that can do some things that the human brain can do, like understand and produce words in a way that sounds like a person, recognise or make images, solve problems, and learn from data fed to software. (Cambridge Dictionary, 2023)

- Credential Stuffing: A type of hack that uses stolen account information, like usernames and passwords that were taken from breaches of other services that are not connected. Over large-scale botnet attacks, the passwords are automatically entered, or "stuffed," into many websites. (Imperva, 2021)

- Password Spraying: As a kind of brute force attack, "password spraying" takes place when an attacker tries to access many accounts using the same password. Many people use obvious and easy-to-guess passwords like "password" or "123456" which makes password spraying attacks successful.

- Brute Force Attacks: According to Kaspersky (2019), A brute force attack uses a method of systematically attempting all possible combinations in order to guess login credentials, encryption keys, or discover a concealed web page. Hackers systematically go through all potential combinations in an attempt to accurately estimate the desired outcome.

- Passwords Entropy: Entropy is a way for determining the quality of a password. The time taken to crack a password indicates how secure the password is. Longer passwords that contain a greater variety of characters have a higher entropy therefore are harder to crack. (Datta, 2022)

- Plan-Do-Check-Act (PDCA) structure: The PDCA/PDSA structure is a continuous process which includes planning, executing, evaluating (or investigating), and taking action. It offers a simple yet effective approach for resolving issues and handling transitions/risks.

- Information Security Management System (ISMS): An information security management system (ISMS) is a set of rules and instructions for keeping private data in an institution secure. The purpose of ISMS is to minimise the risk and keep the business running by avoiding or minimising the effects of a cyber-attack. An ISMS usually looks at how employees act and work, as well as data and technology. It can be aimed at a certain type of data, like customer data, or it can be used all over the company and become part of the way they do things.

- Risk : Risk refers to the possibility that a certain danger may take advantage of a vulnerability in an asset or collection of assets, resulting in the loss or destruction of those assets. Jagodzińska, N. (2022)

- Residual Risk: Residual risk refers to the risk that remains once the risk management procedure has been completed. Jagodzińska, N. (2022)

- Risk Assessment: Risk assessment is the act of evaluating the expected risk against predetermined risk criteria to determine the risk magnitude. Jagodzińska, N. (2022)

- Risk Management: Risk management refers to the coordinated efforts to lead and govern an organisation while considering potential risks. Jagodzińska, N. (2022)

- Collateral: Collateral refers to a technique, procedure, or mechanism that is used to mitigate or minimise risk. Jagodzińska, N. (2022)

Introduction:

People are now a days often calls that data is now new crude oil and it will revolutionize the future same way what crude oil did in past. However with the rise of AI and use of IOT (internet of things), we can say that data is not the crude oil but it the new air. We breathe, generate and consume data through every step we take, and every interaction we participate in though digital gadgets (MCFADIN, 2015). Each click on phone, each step with your phone, you are generating a data and company which own that gadget collects and stores that data with your consent.

Data security is crucial, especially for POS and online hotel booking systems. This section handles sensitive user or company data. Data security while booking hotels online is crucial for user trust and company success. Strong data security is essential to keep online systems working and prevent unwanted access to valuable information.

Data security is crucial for POS systems to protect client payment information and perform smoothly. As online transactions increase, POS terminals become key sites for safeguarding private financial information. Data breaches can result in financial losses, reputation damage, and lawsuits. The integrity and privacy of payment operations must be protected by stringent data security procedures.

Recent events show how serious it is when data security is breached and how open online booking and point-of-sale (POS) systems are to cyber-attacks. For example,

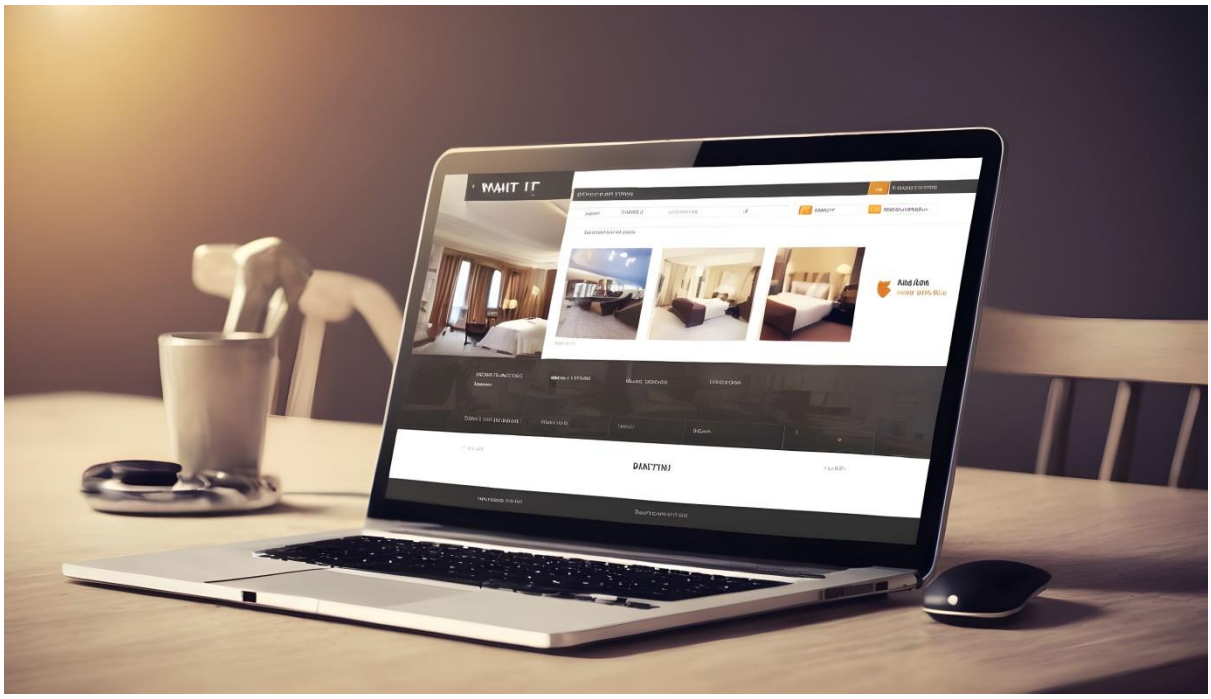
- Due to lake of proper security protocols, Prestige Software, an online hotel reservation platform, suffered a major data breach. Prestige's channel management platform Cloud Hospitality stored millions of hotel customers' names, addresses, and credit card information in a misconfigured Amazon Web Services S3 bucket. The incident affected including, but not limited to Booking.com, Expedia and many other major online booking platforms which uses the Cloud Hospitality as their platform. (Website Planet Security Team, 2020)
- Using point-of-sale (PoS) malware, thieves stole 167k payment records worth over $3M, mostly from US credit cards. (Petkauskas, 2022)

These examples are stark warnings of how important it is to have strong data security means in place to protect online booking and point-of-sale (POS) systems from threats and weaknesses.

This report will examine several factors/roles involved in maintaining data security specific to Online Hotel Booking Systems OR point-of-sale (POS) systems.

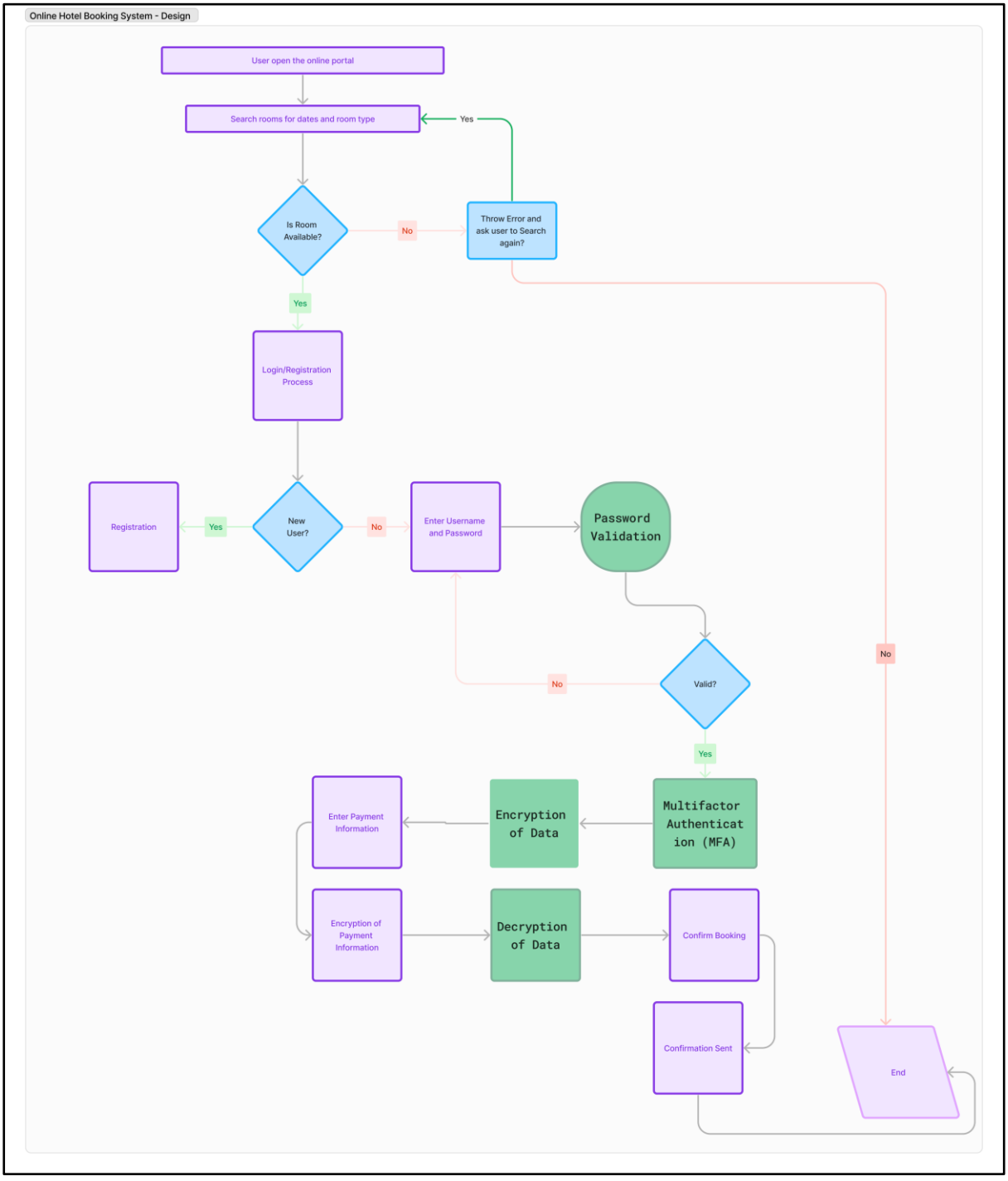
Task 1

Enhancing Security in Online Hotel Booking



1.0 Conceptualization of Online Hotel Booking System:

The flow chart visualizes the process flow of an online hotel booking system, detailing the steps from room search to booking confirmation. It outlines the user journey through various security checks, including password validation, data encryption/decryption, and multifactor authentication, ensuring a secure and efficient online booking experience.



1.1 Password Validation as a Pillar of User Security in Hotel Bookings

Password validation is the process of checking if an elected password meets established criteria regarding its complexity, length, and composition. This involves assessing criteria such as the minimum length of the password, the variety of characters (including uppercase and lowercase letters, digits, and symbols), forbidden patterns (such as dictionary terms or keyboard sequences), and prohibited personal information (like First Name, Date Of Birth etc.).

1.1.1 Rationale for Stringent Password Policies in Online Hotel

According to (Williams, 2023), The latest research indicates that 75% of the global population are not using strong passwords or variants on existing passwords to safeguard their online accounts, and that 64% of the population uses weak passwords or several variations on the same password.

Password validation acts as the initial layer of security against severe authentication vulnerabilities such as credential stuffing, password spraying, and brute force attacks. It ensures;

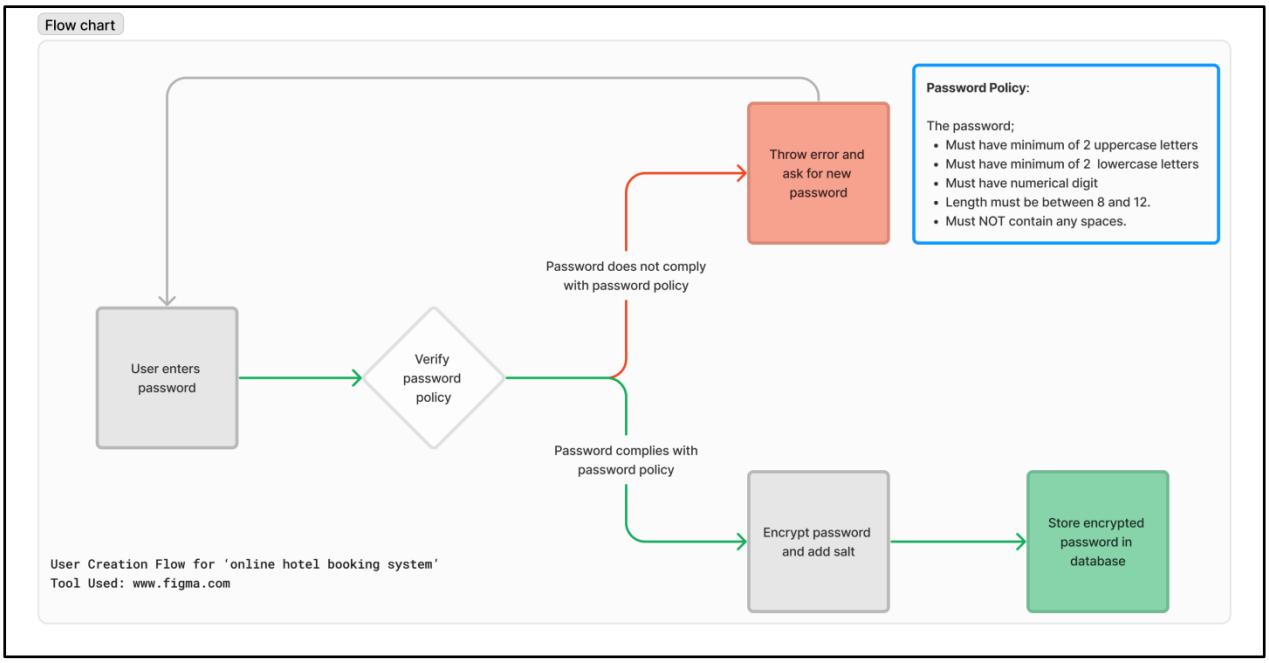
- **Password strength** validation during generation provides password complexity and unpredictability to withstand guessing and brute-force assaults. System should have a policy which ensures High-Entropy Passwords.
- **Reduce the Credential Stuffing Risks**: Checking new passwords against previously disclosed ones reduces credential stuffing, where stolen credentials are used against other sites.
- **Lower Phishing Risks**: Advanced phishing operations target weak passwords. Validated passwords reduce credential theft and account breach.
- **User Awareness and Education**: The validation process teaches users about password hygiene, encouraging stronger passwords and cyber awareness.

1.1.2 The Impact of Insufficient Password Security on online Systems:

Patel and Ling (2020), In August 2020, the Canadian Revenue Agency (CRA) experienced a significant brute-force attack, resulting in unauthorised access to more than 11,000 user accounts. Hackers exploited the GCKey service, a unified digital platform that grants Canadians convenient access to various government services. The hack specifically targeted accounts with vulnerable passwords that had been compromised in previous data breaches or other similar incidents. Using credential stuffing techniques, the hackers attempted to exploit the leaked passwords and successfully gained illegal access to a significant number of GCKey accounts using automated tools. Once the attackers gained access to GCKey, they were able to view a significant amount of personal information from CRA tax records, immigration files, and other services.

This event highlights the significance of implementing policies that enforce password validation and utilise effective hashing methods to prevent credential stuffing and minimise the impact of data breaches.

1.1.3 Visual Guide to Password Validation in Hotel Booking:



When a new user signs up in the hotel booking system, they need to create a password that meets the complexity criteria set in the password policy. The system checks if the policy is met, encrypts the password for security if valid, and stores it to authenticate that user in future.

1.1.4 Python Script for Enforcing Password Rules in Hotel Booking Systems

This `password_validation()` function checks if a given password meets certain criteria. The criteria include length between 8 and 12 characters, at least 2 uppercase letters, at least 2 lowercase letters, no spaces, and at least one digit. If the password meets all the criteria, the function returns True; otherwise, it returns False.

```python
def password_validation(password):

    if len(password) < 8 or len(password) > 12:
        return False
    if sum(1 for c in password if c.isupper()) < 2:
        return False
    if sum(1 for c in password if c.islower()) < 2:
        return False
    if " " in password:
        return False
    if not any(c.isdigit() for c in password):
        return False

    return True
```

Test Case 1: Valid Password

```
#Prompt user to insert the password:
password = input("Enter a password: ")

if password_validation(password):
    print("The password is valid.")
else:
    print("The password is not valid.")
```

```
Enter a password: PassWord1@
The password is valid.
```

Test Case 2: Not Valid Passwords

	Invalid Password	Reason	Screenshot
2	password1	Only 1 capital letter (need at least 2)	Enter a password: password1 The password is not valid.
3	PASSWORD2	Only 1 lowercase letter (need at least 2)	Enter a password: PASSWORD2 The password is not valid.
4	Pass1	Too short (length must be 8-12 chars)	Enter a password: Pass1 The password is not valid.
5	MyPasswordIsVeryLong	Too long (length must be 8-12 chars)	Enter a password: MyPasswordIsVeryLong The password is not valid.
6	Password WithSpace	Contains space (spaces not allowed)	Enter a password: Password WithSpace The password is not valid.
7	password	No number (must contain digit)	Enter a password: password The password is not valid.
8	PASSWORD	No digit/lowercase (need digit & 2+ lowercase)	Enter a password: PASSWORD The password is not valid.

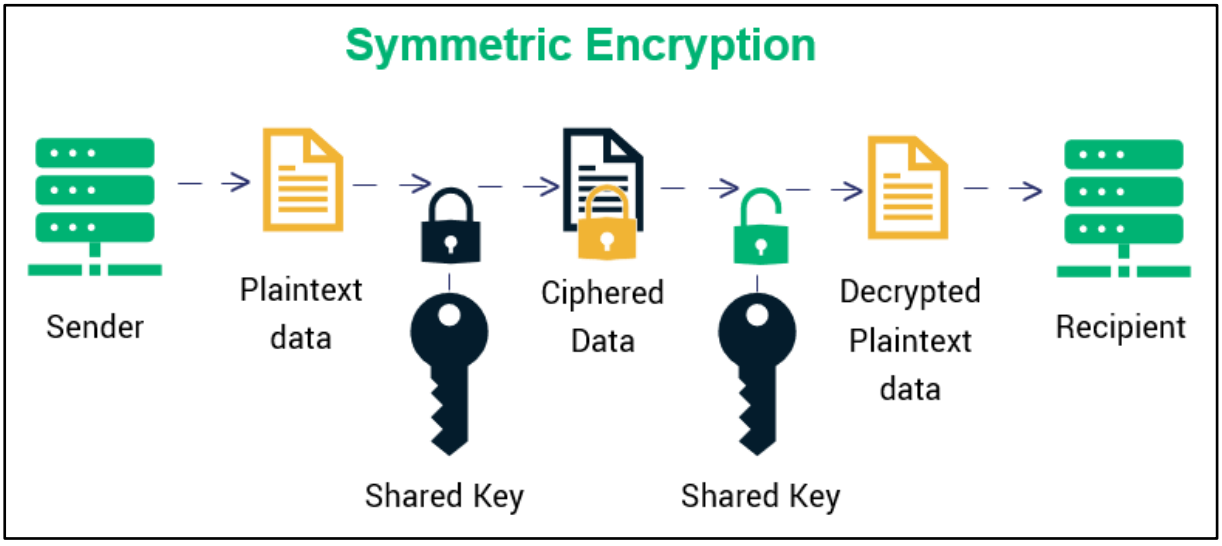
1.2 Ensuring Data Integrity with Encryption in Hotel Booking Transactions

Encrypting data involves transforming a given piece of information into a different form that is not easily recognisable or understandable. The resulting output is referred to as a 'ciphertext'. A 'ciphertext' is created by encrypting data with an algorithm. This method uses random rules to turn the original data into undecipherable data.

The encryption algorithm creates a series of mathematical steps and transforms sensitive data into a secret code. This code can only be decrypted and converted back to plaintext if you possess the knowledge of the rules, also known as a key. The key represents the series of steps the algorithm followed to convert your text into cypher text. Without it, the data cannot be decrypted, ensuring protection against unauthorised access.

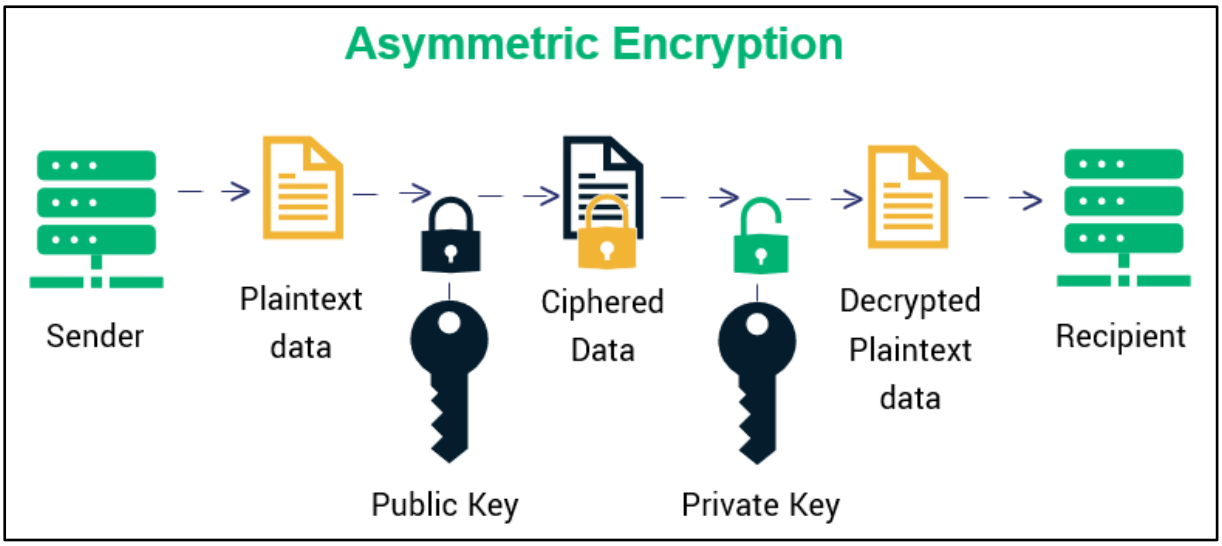
1.2.1 Discussing Encryption and Decryption Strategies for Protecting Hotel Guest Data:

Symmetric Encryption: In Symmetric encryption method, Data gets encrypted and decrypted using only one key. Decrypting information requires the same key as encrypting it. The keys signify a shared secret that two or more individuals can use to keep confidential information. (Taylor et al., 2020, pp.196–201)



Asymmetric Encryption: Asymmetric encryption uses key pairs to differentiate encryption and decryption capabilities, facilitating safe and scalable communication via the design of public key infrastructure (PKI). Public keys can be distributed extensively to facilitate encrypted transmission, but only those in possession of the private keys can decipher the information. (Taylor et al., 2020, pp.196–201)

- The public key is utilised for the purpose of encrypting data. The public key is accessible to anybody for the purpose of encrypting data, which can only be decrypted by the holder of the private key.
- The private key is securely maintained in secrecy by its proprietor. Its purpose is to decipher data that has been encoded using the appropriate public key.



1.2.2 Learning from Failures: How Weak Encryption Affects Hotel Booking Security:

Prestige Software, an online hotel reservation platform, suffered a major data breach. Prestige's channel management platform Cloud Hospitality stored millions of hotel customers' names, addresses, and credit card information in a misconfigured Amazon Web Services S3 bucket without encryption. The incident affected including, but not limited to Booking.com, Expedia and many other major online booking platforms which uses the Cloud Hospitality as their platform. (Website Planet Security Team, 2020)

1.2.3 Python Encryption/Decryption Demonstration for Hotel Booking Confidentiality:

Snippet of Code:

```python
import hashlib
import binascii
import os

def encrypt_password(password):
    salt = hashlib.sha256(os.urandom(60)).hexdigest().encode('ascii')
    pwdhash = hashlib.pbkdf2_hmac('sha512', password.encode('utf-8'), salt, 100000)
    pwdhash = binascii.hexlify(pwdhash)
    return (salt + pwdhash).decode('ascii')

def verify_password(stored_password, provided_password):
    salt = stored_password[:64]
    stored_password = stored_password[64:]
    pwdhash = hashlib.pbkdf2_hmac('sha512', provided_password.encode('utf-8'), salt.encode('ascii'),100000)
    pwdhash = binascii.hexlify(pwdhash).decode('ascii')
    return pwdhash == stored_password
```

`encrypt_password()` function encrypts a password using a salt and PBKDF2 algorithm with SHA-512. The function generates a random salt, derives a hash from the password and salt, and then returns the concatenation of the salt and hash in a printable ASCII format. (Python documentation, 2022) & (Python documentation, 2024)

`verify_password()` function checks a password by comparing a stored password hash with a hash generated from a provided password using a salt and PBKDF2-HMAC algorithm with SHA-512. If

the generated hash matches the stored hash, the function returns True; otherwise, it returns False. (Python documentation, 2022) & (Python documentation, 2024)

Use case 1: Successful Login

```
# Prompt User to input the Password
password = input("Enter a password: ")

#use the encrypt_password function and encrypt the password
hashed_password = encrypt_password(password)
print("Encrypted (hashed) password:", hashed_password)

# Prompt User to input the Password again
password_to_verify = input("Enter the password again for verification: ")

#Using the verify_password function to match both passwords
if verify_password(hashed_password, password_to_verify):
    print("Login successful.")
else:
    print("Login unsuccessful.")
```

```
Enter a password: Test@1234
Encrypted (hashed) password: 5e6d2159549668c6996b8ef01a350fba81b3fc5d976d913cd3c
Enter the password again for verification: Test@1234
Login successful.
```

Use case 2: Unsuccessful Login

```
# Prompt User to input the Password
password = input("Enter a password: ")

#use the encrypt_password function and encrypt the password
hashed_password = encrypt_password(password)
print("Encrypted (hashed) password:", hashed_password)

# Prompt User to input the Password again
password_to_verify = input("Enter the password again for verification: ")

#Using the verify_password function to match both passwords
if verify_password(hashed_password, password_to_verify):
    print("Login successful.")
else:
    print("Login unsuccessful.")
```

```
Enter a password: Test@1234
Encrypted (hashed) password: 1537d5eafd6fe4612ffa3bf9ca50a826c08529c54f60cf97191
Enter the password again for verification: Test@123
Login unsuccessful.
```

1.3 Multifactor Authentication (MFA) as a Defence Strategy in Hotel Booking Systems

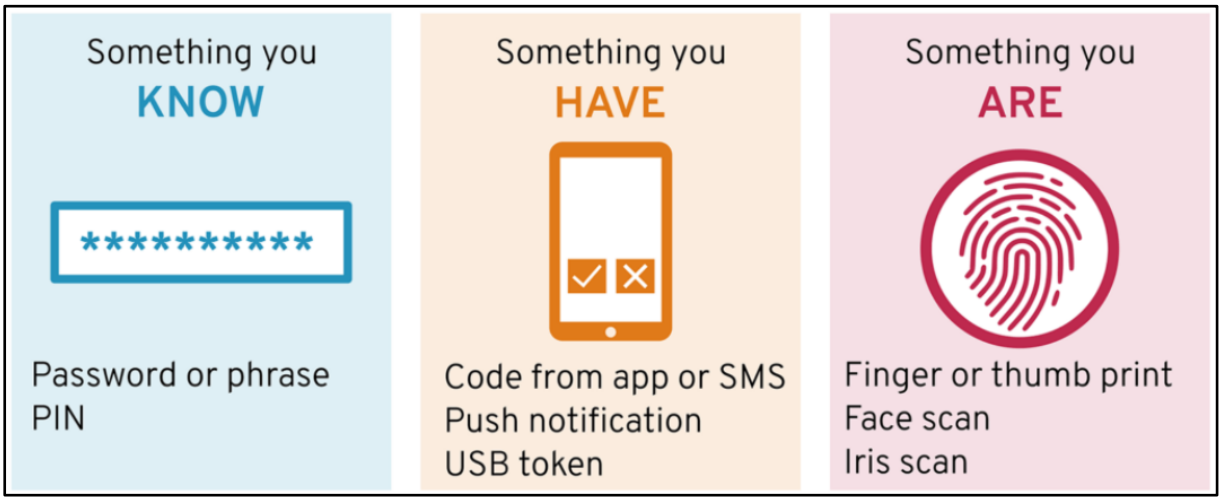
MFA is a crucial security measure for online accounts for Hotel Booking platforms, providing an additional layer of protection beyond passwords. It provides protection against guessing, brute force attacks, and scams can all be done with just a password.

1.3.1 The Critical Role of MFA in Securing Online Hotel Booking Systems:

Multifactor authentication (MFA) is ways to prove who you are that needs two or more proof factors before you can access an account in Hotel Booking system. By needing a second factor, it is much harder for someone who isn't supposed to be there to get in. They would need to have direct access to the other factor even if they got the password.

There are three distinct categories of factors can be used for Multifactor authentications which are:

- Something You Are i.e. Personal identification (e.g., biometric)
- Something you have i.e. Possession (e.g., security token)
- Something you know i.e. Knowledge (e.g., password).



As demonstrated by (Ronn, 2022) on https://www.hsph.harvard.edu

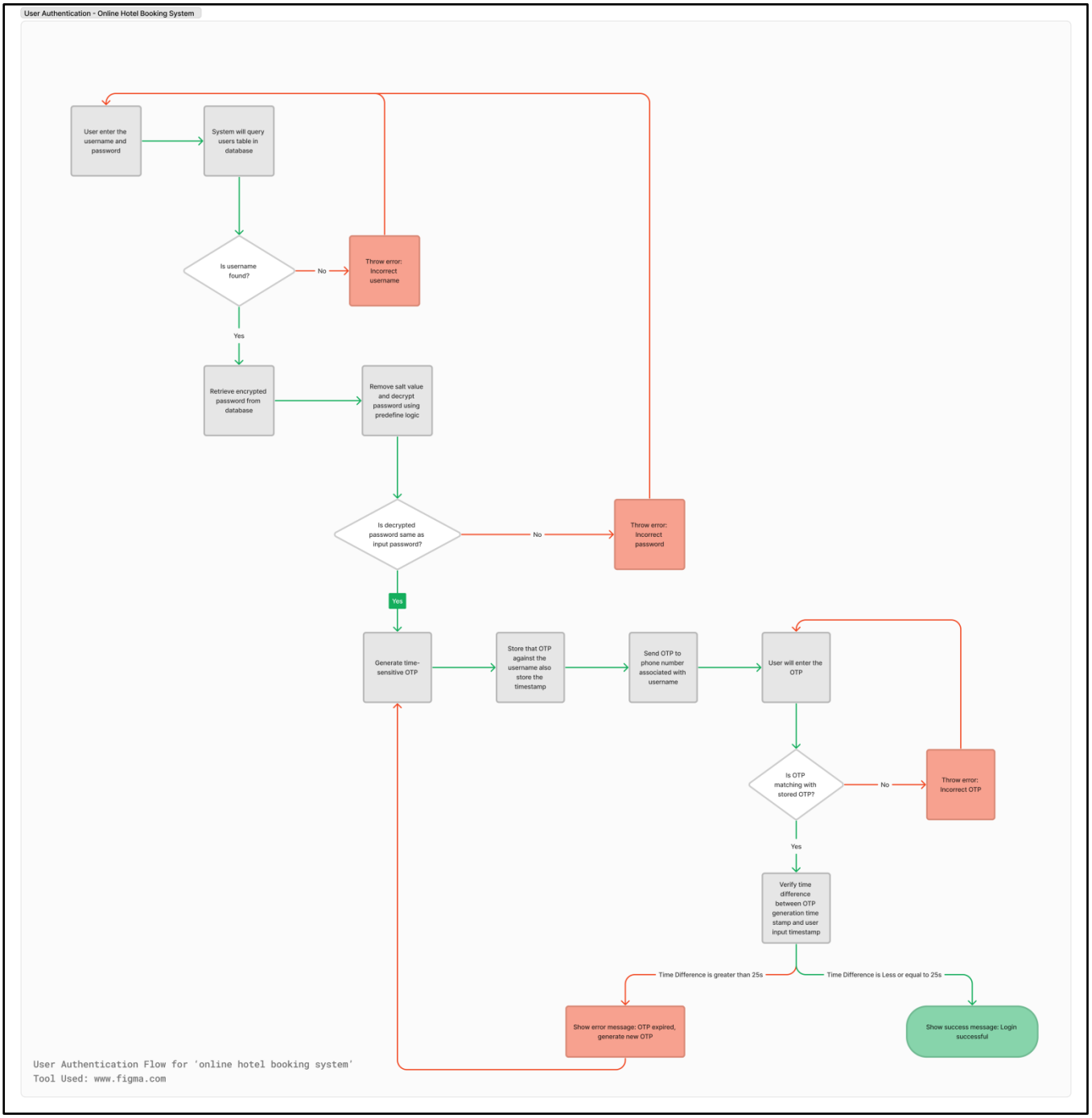
1.3.2 Why Multi-layered Security via MFA is Essential?

The water utilities in the United States, which utilise unitronics programmable logic controllers, experienced a cyber-attack. The operators of these utilities neglected to modify the default passwords for their internet-connected devices, resulting in this breach. This situation could have been prevented by implementing multi-factor authentication or changing the default password. (Brumfield, 2023) & (Cybersecurity and Infrastructure Security Agency CISA, 2023)

1.3.3 MFA Implementation Blueprint for Enhanced Hotel Booking Security:

The diagram below shows the step-by-step process of logging into an online hotel booking system. It begins with the user inputting their username and password. This triggers a series of validation checks. Firstly, the system verifies if the username exists in the database. Then, it retrieves and decrypts the stored password to compare it with the entered password. If the credentials are valid,

the system generates a one-time OTP (One-Time Password) and sends it to the user. The user then enters the OTP. The system checks if the OTP matches and if the time difference since its generation is less than 25 seconds. Finally, the system displays a success message if the login is valid. In case of invalid credentials, incorrect OTP, or expired OTP, the system displays various error messages at different stages of the workflow.



1.3.4 Crafting Python Solutions for MFA in Hotel Booking Systems:

The `generate_otp()` function generates a Time-Based One-Time Password (TOTP). It takes in a secret_key parameter which is the shared secret key used to generate the TOTP. There is also an optional interval parameter which specifies the time interval in seconds for which the TOTP is valid, with a default of 25 seconds.

Inside the function, the current time in seconds since the Unix epoch is obtained using time.time(). This is divided by the interval to get an interval number. This interval number is converted to 8 bytes in big endian byte order. The secret key is then concatenated with the interval number bytes. This concatenated value is hashed using SHA1 to get a 20-byte digest. The last byte of this digest is used to select an offset into the digest. A 4-byte segment starting at the offset is extracted from the digest.

The extracted 4-byte code is converted to an integer. This integer is modulo (%) divided by 1 million to get a 6-digit one-time password code. This TOTP code is returned from the function.

```python
import hashlib
import time

#This function Generates a Time-Based One-Time Password.
def generate_otp(secret_key, interval=25):
    current_timestamp = int(time.time())
    interval_time = current_timestamp // interval
    message = interval_time.to_bytes(8, 'big')
    hmac_result = hashlib.sha1(secret_key + message).digest()
    offset = hmac_result[-1] & 0xf
    code = hmac_result[offset:offset + 4]
    code_int = int.from_bytes(code, 'big')
    otp = code_int % 1000000  # 6-digit code
    return otp

def verify_otp(entered_otp, secret_key, interval=25):
    """Verify the entered OTP."""
    current_otp = generate_otp(secret_key, interval)
    return entered_otp == current_otp

# Secret key for OTP generation
secret_key = b"supersecretkey123"
```

Use case 1 & 2: Correct OTP - Successful Login & Unsuccessful Login

- In first scenario, Time Sensitive One time Password is generated and first the correct OTP was added within 25 second and verified that OPT matched and Login successful.
- In second scenario, Time Sensitive One time Password is generated and first the correct OTP was added after 25 second and verified that OPT matched but Login was unsuccessful because OTP is expired.

```
otp = generate_otp(secret_key)
print("Generated OTP:", otp)

print("Test Case 1: Successful Login - Correct OTP Entered within 25 second")
user_entered_otp = int(input("Enter the OTP: "))
if verify_otp(user_entered_otp, secret_key):
    print("OTP Verified, Login Successfull.")
else:
    print("Verification failed.")

print("Waiting for 26 seconds...")
time.sleep(26)

print("Test Case 2: Unsuccessful Login - Correct OTP Entered after 25 second")
user_entered_otp = int(input("Enter the OTP: "))
if verify_otp(user_entered_otp, secret_key):
    print("Login Successfull.")
else:
    print("OTP is expired. Request New OTP.")
```

```
Generated OTP: 855347
Test Case 1: Successful Login - Correct OTP Entered within 25 second
Enter the OTP: 855347
OTP Verified, Login Successfull.
Waiting for 26 seconds...
Test Case 2: Unsuccessful Login - Correct OTP Entered after 25 second
Enter the OTP: 855347
OTP is expired. Request New OTP.
```

Use Case 3: Incorrect OTP - Unsuccessful Login

```
otp = generate_otp(secret_key)
print("Generated OTP:", otp)

print("Test Case 3: Unsuccessful Login - Incorrect OTP Entered.")
user_entered_otp = int(input("Enter the OTP: "))
if verify_otp(user_entered_otp, secret_key):
    print("OTP Verified, Login Successfull.")
else:
    print("Incorrect OPT, Enter the Correct OTP.")
```

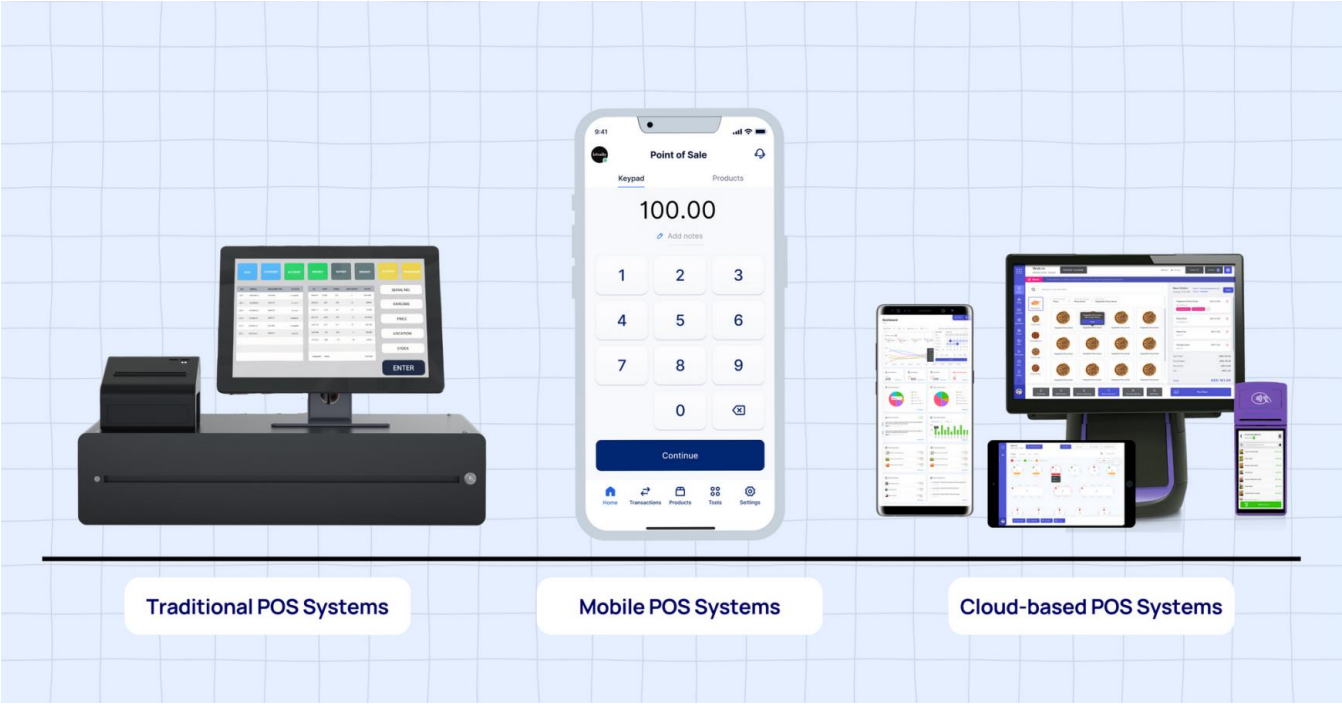
```
Generated OTP: 940844
Test Case 3: Unsuccessful Login - Incorrect OTP Entered.
Enter the OTP: 940843
Incorrect OPT, Enter the Correct OTP.
```

1.4 Conclusion

This assessment has successfully demonstrated the critical importance and application of data security measures in the context of an online hotel booking system. The combination of these security measures meets the growing demand for strong cyber security systems in the face of rising online threats and vulnerabilities. By implementing these tactics, the system not only secures and protects user data, but it also improves the online platform's general trustworthiness and dependability. This evaluation emphasises the importance of on-going monitoring and the implementation of sophisticated security procedures in the digital world, particularly for systems that handle sensitive user information.

Task 2

ISO 27001 & PCI DSS Framework w.r.t. POS System



2.1 Introduction

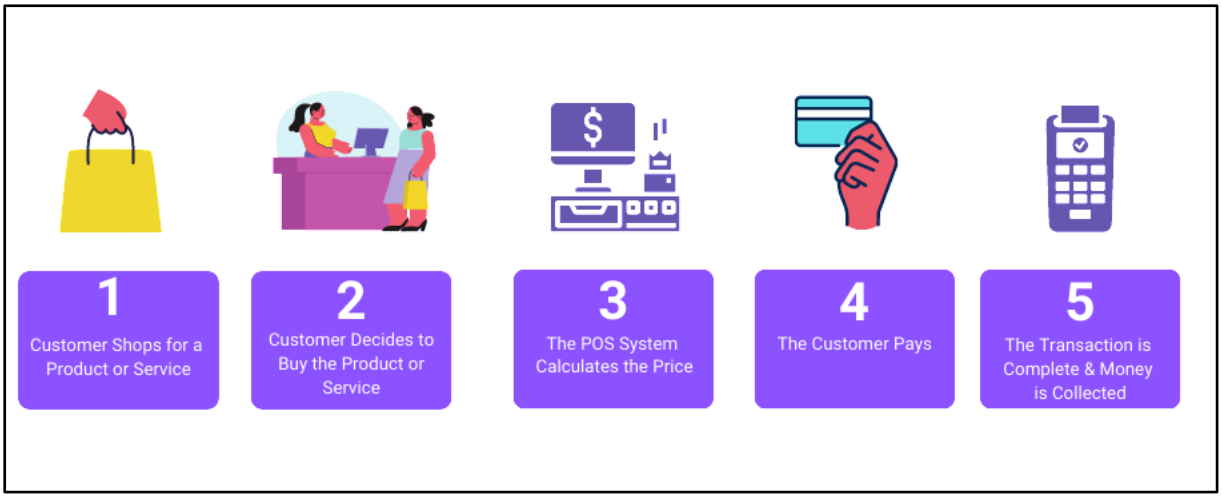
Mobile phone payment systems, NFC (near field communication) enabling contactless transactions, and card readers have made purchases possible anywhere in the retail business. These improvements bring vulnerabilities that put data security and privacy at risk. ISO 27001 and PCI DSS give extensive safeguards to mitigate these issues. ISO 27001's holistic information security management and PCI DSS's payment card security focus protect current POS systems from dangers. Organisations may secure sensitive data, preserve consumer confidence, and meet legal and regulatory requirements by following these guidelines.

2.1.1 What is POS Systems?

According to (Peek, 2017), POS short for point-of-sale system, is a combination of hardware and software that retailers, restaurants, and other businesses use to conduct sales transactions. POS systems offers comprehensive features for business management, such as payroll, loyalty programs, inventory tracking, and employee scheduling, aimed at improving efficiency at both the front end and back office.

2.1.2 How does a POS system work?

Per (Crawford, Anthony and Orem, 2021), A point of sale (POS) system computes the total cost of a customer's purchase, incorporates the applicable sales tax, facilitates the payment process, and records the precise time and date of the transaction. Upon finalising the transaction, several point-of-sale (POS) systems provide both a physical and/or electronic receipt, while also updating inventory information.



As illustrated by (360Connect, 2024), on https://www.360connect.com/

2.2 Literature Review of frameworks

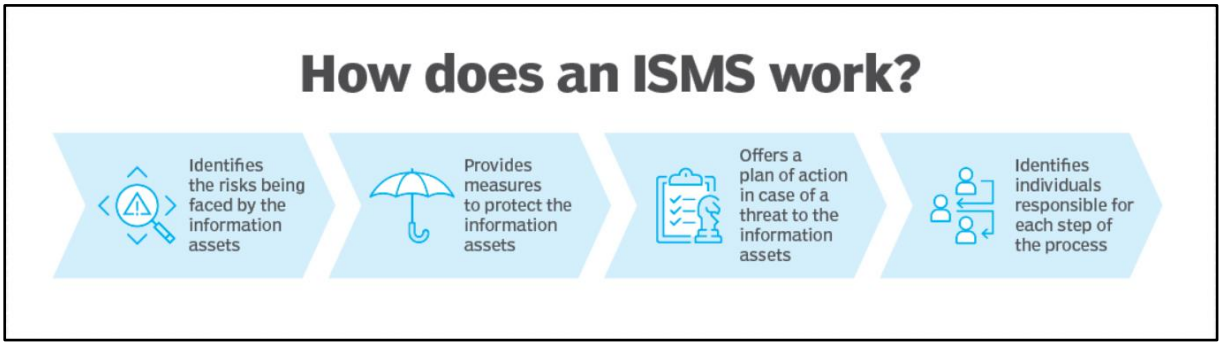
2.2.1 ISO 27001:2022 – ISMS Policy – Requirements & Controls

ISO 27001: 2022 is the latest version of the ISO/IEC 27001 international standard specifying requirements for information security management systems (ISMS) defined by International Organization for Standardization(ISO). iso.org (2023)

Accordingly to (Calder and Watkins, 2015, p.40), ISO 27001 Framework is built upon the Plan-Do-Check-Act (PDCA) structure, which offers an on-going process for executing, upholding, and enhancing the Information Security Management System (ISMS). It encompasses the following fundamental principles:

- Plan - Risk assessment and mitigation: Identify potential risks
- Do - Risk Mitigation: Adopt security measures to address and minimise such risks. Generally controls are chosen from ISO 27002 in accordance with the specific needs of the company.
- Check - Management commitment: Senior management must demonstrate a firm dedication to defining policy, objectives, allocating resources, and conducting regular reviews of the Information Security Management System (ISMS).
- Act – Continuous improvement: The repetition of the PDCA cycle allows for the identification of flaws and the implementation of improvements.

In order to comply with 27001:2022 standards, an organisation must have an information security management system policy that considers the business's nature, the organisation itself, its location, and its assets. The ISMS Policy must be approved and promote by the management, effectively conveyed to employees and responsible parties, and implemented accordingly.



Note: Refer the **Appendix A** for ISMS Policy checklist which I have created by understanding ISO 27001 framework.

2.2.2 PCI DSS: Payment Card Industry Data Security Standard

In the past few years, the payment card business has dealt with the issue of who is responsible for charges that were not authorised. Identity theft and the use of personal information for illegal purposes, on the other hand, poses new risks to users and those who benefit from their use, such as retailers, banks, and payment card companies.

Payment Card Industry–Digital Security Standard (PCI–DSS) sets general security standards that give private organisations the freedom to put in place and customise security measures that are unique to their own operations in order to keep payment account data safer. With the help of clear and straightforward rules and questionnaires, it takes a practical approach to implementing information security. The standard was made by American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc., which are some of the original payment brands of the PCI Security Standards Council. Gikas, C. (2010)

PCI-DSS principles and requirements: (PCI Security Standards Council, 2023)

Principle	Requirement
1. Build and Maintain a Secure Network	Requirement 1: Install and maintain a firewall configuration to protect cardholder data
	Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters
2. Protect Cardholder Data	Requirement 3: Protect stored cardholder data
	Requirement 4: Encrypt transmission of cardholder data across open, public networks
3. Maintain a Vulnerability Management Program	Requirement 5: Use and regularly update anti-virus software
	Requirement 6: Develop and maintain secure systems and applications
4. Implement Strong Access Control Measures	Requirement 7: Restrict access to cardholder data by business need-to-know
	Requirement 8: Assign a unique ID to each person with computer access
	Requirement 9: Restrict physical access to cardholder data
5. Regularly Monitor and Test Networks	Requirement 10: Track and monitor all access to network resources and cardholder data
	Requirement 11: Regularly test security systems and processes
6. Maintain an Information Security Policy	Requirement 12: Maintain a policy that addresses information security

2.3 Use Case Discussion POS Security:

Tackling vulnerabilities in present-day point-of-sale systems demands an in-depth knowledge with particular risks as well as the implementation of targeted controls drawn from industry standards derived from frameworks such as PCI DSS and ISO 27001. Below are the some use cases;

Use Case 1. Enhancing Security for Remote Transaction Processing

Mobile point-of-sale (POS) tools have made it much easier to do business from a distance. However, this ease of use comes with a higher chance of data being stolen while being sent.

- Clause A.13.2.1 of ISO 27001 suggests putting in place strict Information Transfer Policies and Procedures to protect against these risks. In order to do this, safe routes for data transmission must be set up and information transfer methods must be strong against being hacked or accessed without permission. iso.org (2023)
- PCI DSS Requirement 4 stresses how important it is to secure customer data when it is sent over open, public networks. It is very important to use encryption to keep private data safe while it is being sent, especially over networks that can be accessed by people who aren't supposed to. PCI Security Standards Council (2022)

Use Case 2. Securing Mobile Devices in POS Systems

Mobile devices used for transactions create risks, like losing or being stolen that could allow unauthorised people to access private information

- ISO 27001 includes several sections, such as A.11.2.8 (Clear Desk and Clear Screen Policy), A.11.1.5 (Working in Secure Areas), and A.6.2 (Mobile Devices and Teleworking), that explain how to keep mobile devices and the places where they work safe. As a result of these instructions, steps like secure device management, data encryption, and access limits should be taken. iso.org (2023)
- PCI DSS Requirement 9 is also about limiting physical access to user data. This makes it even more important to protect the physical devices against loss or unauthorised access. PCI Security Standards Council (2022)

Use Case 3. Mitigating Risks Associated with Public Wi-Fi Networks

Mobile devices used for transactions create risks, like losing or being stolen that could allow unauthorised people to access private information

- ISO 27001 includes several sections, such as A.11.2.8 (Clear Desk and Clear Screen Policy), A.11.1.5 (Working in Secure Areas), and A.6.2 (Mobile Devices and Teleworking), that explain how to keep mobile devices and the places where they work safe. As a result of these instructions, steps like secure device management, data encryption, and access limits should be taken. iso.org (2023)
- PCI DSS Requirement 9 is also about limiting physical access to user data. This makes it even more important to protect the physical devices against loss or unauthorised access. PCI Security Standards Council (2022)

Use Case 4. Protecting Against Malware and Phishing Attacks

Malware and hacking attempts specifically target point-of-sale systems that are run on smartphones and other mobile devices. People behind these hacks want to steal private information and damage the integrity of data.

- Clause A.12.2.1 (Controls against Malware) in ISO 27001 tackles this danger by requiring protection measures against malicious software to be put in place. iso.org (2023)
- PCI DSS adds to this method with Requirement 5, which says that all systems must be protected against malware by keeping their antivirus software up to date. This makes sure that POS systems are safe from these kinds of dangers. PCI Security Standards Council (2022)

Use Case 5. Ensuring the Security of Third-party Service Providers

Additional dangers arise from relying on third-party programmes and services, as these suppliers have differing security standards.

- To ensure that third-party suppliers follow the organization's security requirements, clause A.15.1.1 (Information Security Policy for Supplier Relationships) of ISO 27001 stresses the need of strict security rules controlling supplier contacts. iso.org (2023)
- To make sure that even service providers effectively safeguard sensitive payment card information, PCI DSS Requirement 12.8 expands this to include the administration and monitoring of service providers' compliance with PCI DSS. PCI Security Standards Council (2022)

By integrating these detailed approaches and adhering to the specific clauses and requirements of ISO 27001 and PCI DSS, organizations can enhance the security and integrity of their POS systems. This comprehensive framework ensures the protection of sensitive.

2.4 Conclusion:

The fast development of point-of-sale (POS) systems has created new security holes, making it even more important to have strict security measures. The combination of ISO 27001 and PCI DSS guidelines provides a complete method for lowering these risks, protecting private data, and keeping customers' trust. Modern point-of-sale (POS) systems pose security challenges. ISO 27001's strategy approach and PCI DSS's focus on payment security offer practical ways to deal with these issues. According to these guidelines, businesses can improve their security, protect themselves from possible threats, and meet legal requirements. These strong information security and payment card protection practices must be actively adopted by businesses in the retail and service sectors in order to ensure safe operations in the future.

Appendix: A – ISMS Policy example

Here I have created a ISMS format and added the use case related to POS system and drafted checklist for each stage w.r.t. requirement of ISO 27001 / 2022 clauses;

Phase 1. Risk Identification

- ISO 27001:2022 Clause 6.1.2 – Information security risk assessment
- ISO 27001:2022 Clause 8 - Operational Planning and Control
- ISO 27001:2022 Clause 8.2.1 Information security risk identification

Use Case No	(1) Activity/ Asset/ Function related to Information (Hardware, Software, Digital Information)	(2) Description of Issue (Confidentiality, Integrity or Availability)	(3) Risk to Business (Revenue/Reputation/ Regulatory, Loss of Data etc.)	(4) Existing Controls if any (Annexure A of ISO 27001 or Others)Restricted access to authorized employees
1	Access of POS System / Sharing Credentials	Integrity & Confidentiality- Unauthorized access to POS System will breach the Integrity of data	Data Confidentiality and integrity breach which lead to Regulatory actions or tarnish to Reputation.	1. Restricted access to only limited users. 2. Multi Factor Authentication in place which also has biometric authentication 3. Clean Desk Policy to ensure no one keeps the confidential data which can be access by unauthorized person.
2	Hardware-Loss Of Data/ Drive Corruption, Automatic damage/Life for digital devices	Availability - System crash/auto shutdown and data stored on POS gets deleted and could not recover.	Leads to Loss of Revenue and lead to compliance issues, customer dissatisfaction	1. Auto backup protocol in place to store the session data directly on cloud to ensure that no data lost. 2. Power Backup is also available at each location where POS Systems is being used. 3. System available to clone the existing POS access point in to new digital device instantaneously
3	Virus / Malware Threats	Integrity & Availability: Data Theft, misuse of data by potential hacker or denial-of-service.	Loss of Revenue and lead to compliance issues	1. POS will connect to database with use of VPN setup by company. 2. Endpoint protection installed on POS to disable all input or output ports. 3. Antivirus installed in each POS and Firewall in place. 4. Mandatory information security certification for each employee of organization. 5. Access to website other than company approved list of website is blocked.
4	POS Skimming/Point-of-Sale Devices tempered	Data breach, Unauthorized access to POS System will breach the Integrity of data	Data Confidentiality and integrity breach which lead to Regulatory actions or tarnish to Reputation.	1. Daily checklist in place which is followed by employee while starting POS to look for foreign device. 2. POS system has inbuilt protocol to scan for foreign device attached to POS. 3. Installation of any new software can be done by IT Team after getting clearance from Information Security Team.

Phase 2. Risk Analysis & Risk Evaluation

- Clause 8.2.2 - Information security risk analysis
- Clause 8.2.3 - Information security risk evaluation

Company can define the Significant Risk Threshold based on their nature of business. Here I have define it as 9 to evaluate the risk. So any use case which has the (7) risk value above 9 must have 'Phase 3 Risk Mitigation' available to ensure such risks never arises.

Use Case No	(5) Severity of Consequence in case control fails/ absent (on Scale of 1 to 5)	(6) Probability or Likelihood of Risk Occurring post current control established	(7) Risk Value (Severity x Likelihood)	(8) Significant Risk (Action Mandatory)
1	5	1	5	No
2	5	2	10	Yes
3	4	2	10	Yes
4	5	1	5	No
		(13) Significant Risk Threshold	9	

Phase 3. Risk Mitigation

- ISO 27001:2022 A.6.1 Internal organization
- ISO 27001:2022 A.6.1.1 Information Security Roles and Responsibilities

Use Case No	(1) Activity/ Asset/ Function related to Information (Hardware, Software, Digital Information etc.)	(8) Significant Risk (Action Mandatory)	(9) Proposed Controls/Target Time Actions for Significant Risk	(10) Target Time frame for completion of the action	(11) Risk Owner (Who will ensure action will be taken)	(12) Status (Completed, Scheduled, WIP, Other)
1	Access of POS System / Sharing Credentials	No	-	-	-	-
2	Hardware-Loss Of Data/ Drive Corruption, Automatic damage/Life for digital devices	Yes	Define life span for each digital device used in architecture. Audit the hardware assets for out-dated inventory. Audit the data log and search for abnormality	Every Quarter	Information Security Team	Scheduled
3	Virus / Malware Threats	Yes	Scan all the POS to update the antivirus database and scan for abnormality	Every Week	Information Security Team	Scheduled
4	POS Skimming/Point-of-Sale Devices tempered	No	-	-	-	-

References:

- World Economic Forum. (2024). Global Risks Report 2024 | World Economic Forum. [online] Available at: https://www.weforum.org/publications/global-risks-report-2024/in-full/ [Accessed 20 Jan. 2024].
- Carballo, R. (2024). Data Breach at 23andMe Affects 6.9 Million Profiles, Company Says. The New York Times. [online] 4 Dec. Available at: https://www.nytimes.com/2023/12/04/us/23andme-hack-data.html [Accessed 20 Jan. 2024].
- Cambridge Dictionary, 2023, ARTIFICIAL INTELLIGENCE | definition in the Cambridge English Dictionary. [online] Available at: https://dictionary.cambridge.org/us/dictionary/english/artificial-intelligence [Accessed 20 Jan. 2024].
- Patel, R. and Ling, P. (2020). CRA shuts down online services after thousands of accounts breached in cyberattacks. [online] CBC. Available at: https://www.cbc.ca/news/politics/canada-revenue-agency-cra-cyberattack-1.5688163 [Accessed 20 Jan. 2024].
- Petkauskas, V. (2022). Details of 160k stolen US cards found online | Cybernews. [online] Cybernews. Available at: https://cybernews.com/news/160k-stolen-us-credit-cards/ [Accessed 5 Feb. 2024].
- Website Planet Security Team (2020). Report: Hotel Reservation Platform Leaves Millions of People Exposed in Massive Data Breach. [online] Website Planet. Available at: https://www.websiteplanet.com/blog/prestige-soft-breach-report/ [Accessed 5 Feb. 2024].
- keepersecurity.com (n.d.). What Is Password Spraying? | Keeper. [online] www.keepersecurity.com. Available at: https://www.keepersecurity.com/en_GB/threats/password-spraying-attack.html [Accessed 20 Jan. 2024]. What is Password Spraying?
- imperva.com (2023). What is Credential Stuffing | Attack Example & Defense Methods | Imperva. [online] www.imperva.com. Available at: https://www.imperva.com/learn/application-security/credential-stuffing/ [Accessed 20 Jan. 2024]. What Is Credential Stuffing?
- Kaspersky (2019). Brute force attack: Definition and examples. [online] Kaspersky.com. Available at: https://www.kaspersky.com/resource-center/definitions/brute-force-attack [Accessed 20 Jan. 2024]. What's a Brute Force Attack?
- Datta, S. (2022). How to Determine the Entropy of a Password? | Baeldung on Computer Science. [online] www.baeldung.com. Available at:

https://www.baeldung.com/cs/password-entropy [Accessed 20 Jan. 2024]. Password Strength with Cracking Odds.

- 360Connect. (2024). How Does a Restaurant POS System Work? [online] Available at: https://www.360connect.com/product-blog/how-does-a-restaurant-pos-system-work/ [Accessed 22 Jan. 2024].
- Crawford, H., Anthony, L. and Orem, T. (2021). What Is a Point-of-Sale (POS) System and How Does it Work? [online] NerdWallet. Available at: https://www.nerdwallet.com/article/small-business/what-is-a-pos-system#:~:text=THISSmall%20Business-,What%20is%20a%20POS%20system%3F,customer%20conduct%20a%20retail%20transaction. [Accessed 22 Jan. 2024].
- iso.org (2023). ISO/IEC 27001:2022. [online] https://www.iso.org/standard/27001. Available at: https://www.iso.org/standard/27001 [Accessed 22 Jan. 2024].
- Jagodzińska, N. (2022) 'Information Security Management in Crisis (Ismc) According to the Standard Pn- Iso/Iec 27001: 2017. Introduction to Useful of the System in Small and Medium Enterprises (Sme)', Scientific Papers of Silesian University of Technology. Organization & Management / Zeszyty Naukowe Politechniki Slaskiej. Seria Organizacji i Zarzadzanie, (163), pp. 123–131. doi:10.29119/1641-3466.2022.163.7. [Used https://research.ebsco.com/ to access the article]
- Calder, A. and Watkins, S. (2015). IT governance: an international guide to data security and ISO 27001/ISO 27002. 6th Edition ed. London: Koganpage, p.40. Continual improvement, Plan–Do–Check–Act, and process approach.
- Gikas, C. (2010) 'A General Comparison of FISMA, HIPAA, ISO 27000 and PCI-DSS Standards', Information Security Journal: A Global Perspective, 19(3), pp. 132–141. doi:10.1080/19393551003657019.
- Engle, M. (2024). Council Post: Using PCI DSS V4.0 To Modernize Identity Frameworks And Controls. [online] Forbes. Available at: https://www.forbes.com/sites/forbestechcouncil/2024/01/17/using-pci-dss-v40-to-modernize-identity-frameworks-and-controls/ [Accessed 23 Jan. 2024].
- PCI Security Standards Council (2022). Document Library. [online] PCI Security Standards Council. Available at: https://www.pcisecuritystandards.org/document_library/?category=pcidss&document=pci_dss [Accessed 23 Jan. 2024].

- Python documentation. (2022). hashlib — Secure hashes and message digests. [online] Available at: https://docs.python.org/3/library/hashlib.html [Accessed 25 Jan. 2024].
- Python documentation. (2024). time — Time access and conversions. [online] Available at: https://docs.python.org/3/library/time.html [Accessed 25 Jan. 2024].
- Python documentation. (2024). binascii — Convert between binary and ASCII. [online] Available at: https://docs.python.org/3/library/binascii.html [Accessed 25 Jan. 2024].
- Ronn, M. (2022). Cybersecurity Month: Multi-Factor Authentication (MFA). [online] Department of Information Technology. Available at: https://www.hsph.harvard.edu/information-technology/2022/10/03/october-is-cybersecurity-month-week-1/ [Accessed 21 Jan. 2024]. The 3 Factors of MFA.
- Brumfield, C. (2023). Water system attacks spark calls for cybersecurity regulation. [online] CSO Online. Available at: https://www.csoonline.com/article/1255839/water-system-attacks-spark-calls-for-cybersecurity-regulation.html [Accessed 21 Jan. 2024].
- Cybersecurity and Infrastructure Security Agency CISA. (2023). IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including U.S. Water and Wastewater Systems Facilities | CISA. [online] Available at: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-335a [Accessed 21 Jan. 2024].
- Peek, S. (2017). Types of POS Systems. [online] business.com. Available at: https://www.business.com/articles/types-of-pos-systems/ [Accessed 22 Jan. 2024].
- Taylor, A., Alexander, D., Finch, A. and Sutton, D. (2020). Information security management principles. 3rd edition. ed. London: Bcs, pp.196–201. Basic cryptographic theory, techniques and algorithm types.
- Ncsc.gov.uk. (2024). MOVEit vulnerability and data extortion incident. [online] Available at: https://www.ncsc.gov.uk/information/moveit-vulnerability [Accessed 21 Jan. 2024].