CARDIFF SCHOOL OF TECHNOLOGIES

4D Digidol | Data | Dylunio | Dyfodol

Cardiff Metropolitan University	
Cardiff School of Technologies	
Academic Year : 2023/2024	
Term 2	
Module Name :	Information Security
Module Code :	CIS7028
Module Leader :	Dr Liqaa Nawaf
MSc Program :	MSc Data Science
Assignment Title :	Information Security Assignment
Student Name :	Aaditya Vengatachalapathy
Student Id :	st20290358

Table Of Contents

List of Figures

List Of Abbreviations

- **PbDD** – Data Protection by Design and Default
- **GDPR** – General Data Protection Regulation
- **PDPA** – Personal Data Protection Act
- **NIST** – National Institute of Standards and Technology
- **SIEM** – Security Information and Event Management
- **CCTV** – Closed Circuit Television
- **CISO** – Chief Information Security Officer
- **MFA** – Multi – Factor Authentication
- **RBAC** – Role Based Access Control
- **PII** – Personal Identifiable Information
- **TLS** – Transport Layer Security
- **IDPS** – Intrusion Detection and Prevention
- **COBIT** – Control Objectives for Information and Related Technologies
- **ISO27001** – Information Security Standards published by International Organization Standardization (ISO).

Chapter – 1

1.1 Introduction

The assignment focuses on developing surveillance technologies (CCTV, Face Recognition) and contact tracing applications for the UK government. This study offers a thorough plan based on Data Protection by Design and Default (PbDD) principles, ensuring that both priorities are ensured here.

1.1.1 Data Protection

PbDD serves as the foundation for this report.

Privacy by Design: A Change in Perspective Imagine a future in which privacy is the default setting. Users should not have to navigate complex menus to opt out of data collecting. This empowers people by giving them control of their data from the start(ICO, 2023).

Minimalism as a Guiding Principle: Not all data is created equally. CCTV footage can be anonymised whenever possible, hiding faces while recording important location data for contact tracking. This reduces the amount of sensitive data collected, lowering the risk of a security compromise (ICO, 2023).

Transparency: Knowledge is power. A user-friendly and thorough privacy policy will be easily accessible through the application. This policy should be stated in clear, straightforward language that everyone can comprehend. It will specify what information is gathered, how it is utilised, and for how long. Empowering users with knowledge develops trust and gives them control over their information (ICO, 2023).

1.1.2 Aligning with UK GDPR

The technology should follow the established politicized framework of the UK General Data Protection Regulation (GDPR). This framework establishes guidelines for data collection, storage, and use. Ensuring compliance with the UK GDPR is critical for numerous reasons:

Justification for processing: Respecting user rights. We cannot collect data on a whim. Processing user data requires a clear and legal basis, such as consent, a contractual duty, or a crucial public interest, such as preserving public health during pandemic (ICO, 2018).

Respecting User Rights: Put Users in Control Users have control over their data. We must ensure that they have the right to access, rectify, erase, and restrict the processing of personal data, as defined in the UK GDPR. This empowers individuals by allowing them to handle their own information and builds trust in the system (ICO, 2018).

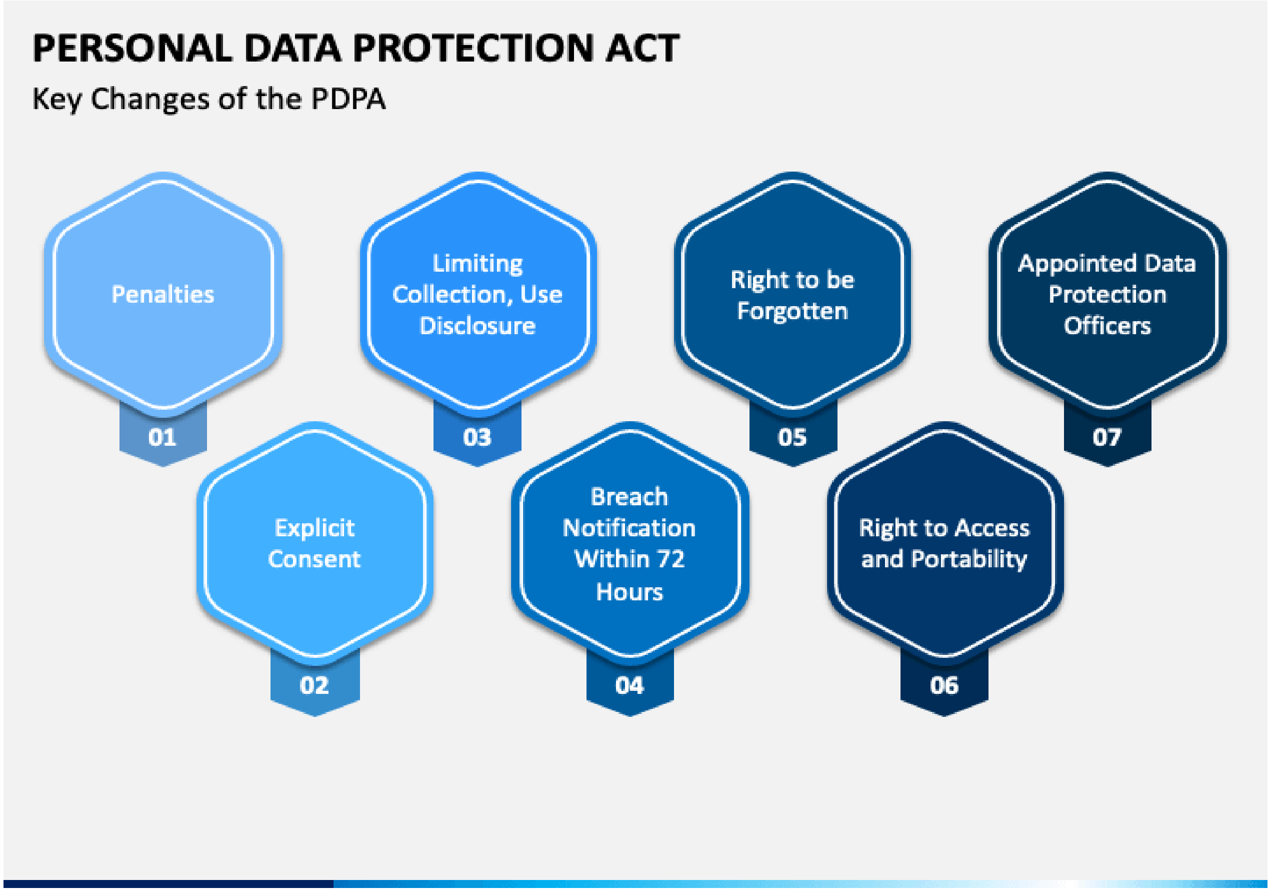
Data Minimization in Action: The UK GDPR promotes the "less is more" approach. We must acquire only the data required for our stated purpose while avoiding acquiring superfluous personal information. This limits the quantity of data at risk in the event of a security compromise and alleviates potential privacy concerns (ICO, 2018).

1.1.3 Safeguarding Privacy in Practice

Meaningful Consent: We must give clear and simple information about data collecting procedures before requesting consent. Users should understand what they are consenting to and feel free to decline(Information Commissioner's Office, 2012).

Anonymization and pseudonymization: Balancing needs and privacy. When possible, data should be anonymized to protect user identity. Pseudonymization can be utilised in situations requiring some identification . In this case, data is associated with a pseudonym rather than a specific individual. This decreases the danger of revealing sensitive information while yet allowing for contact tracking operations (Information Commissioner's Office, 2012).

Data Lifecycle Management: Responsible Stewardship. Data should not remain indefinitely. We require explicit policies regarding data keeping and destruction. Data should only be kept for as long as is absolutely necessary (Information Commissioner's Office, 2012).



PERSONAL DATA PROTECTION ACT

Key Changes of the PDPA

01 Penalties

02 Explicit Consent

03 Limiting Collection, Use Disclosure

04 Breach Notification Within 72 Hours

05 Right to be Forgotten

06 Right to Access and Portability

07 Appointed Data Protection Officers

Figure 1 - PDPA Insights to Data Protection

1.2 Mapping Best Practices with GDPR

Developing CCTV or Face Recognition technology for public health requires a delicate balance of strong security and strict data protection rules. Here's a detailed look at how best practices from ISO 27001, Cyber Essentials Plus, NIST Cybersecurity Framework (CSF), and COBIT may be strategically aligned with the UK GDPR to create a secure and privacy-docile solution.

1.2.1 Protection by Design and Default (PbDD)

ISO 27001: This internationally recognised standard emphasises risk management, which naturally encourages the discovery and mitigation of privacy threats. Annexe A, a treasure trove of security measures, gives recommendations on access control, data encryption, and user awareness, all of which are critical parts of data security (A.5 INFORMATION SECURITY POLICIES A.5.1 Management direction of information security A.5.1.1 Policies for Information Security - A.5.1.2 Review of the policies for information security - ISO 27001 CONTROLS A.6 ORGANZATION OF INFORMATION SECURITY, n.d.).

Cyber Essentials Plus: This UK government-supported project focuses on technical security controls such as boundary firewalls and patch management. These controls are critical for protecting acquired data from unauthorised access, which is a key principle of PbDD (Irwin, 2021).

NIST CSF: This comprehensive methodology from the National Institute of Standards and Technology provides an organised approach to controlling cybersecurity threats. The "Protect" function then directs the creation of safeguards to mitigate those risks, ensuring that data protection is prioritised throughout the development process (www.ncsc.gov.uk, 2022).

COBIT: This IT governance framework outlines a strategy for incorporating data security and privacy concerns throughout the project lifecycle. Its "Align, Plan, and Organise" domains emphasise the significance of complying with relevant standards such as the UK GDPR from the outset. This guarantees that PbDD principles are included into the project's planning and execution (www.onetrust.com, n.d.).

1.2.2 Outline of GDPR and it's functionalities

The UK GDPR sets standards for data pre-processing, and these frameworks might be helpful in achieving the docility.

ISO 27001: This standard emphasises accountability with its "Management Responsibility" provision. This confirms top management's commitment to data privacy and actively supports compliance with the UK GDPR(A.5 INFORMATION SECURITY POLICIES A.5.1 Management direction of information security A.5.1.1 Policies for Information Security - A.5.1.2 Review of the policies for information security - ISO 27001 CONTROLS A.6 ORGANZATION OF INFORMATION SECURITY, n.d.).

Cyber Essentials Plus: This project promotes technical compliance by focusing on safeguards that address data breaches, which are a major concern under the UK GDPR. Implementing these procedures can greatly minimise the risk of breaches while also demonstrating a commitment to data security(ICO, 2018)..

NIST CSF: The NIST CSF outlines a structured strategy to installing data security policies and conducting privacy impact assessments (PIAs). PIAs are essential under the UK GDPR because they assist organisations in identifying and mitigating privacy risks connected with data processing operations(ICO, 2023).

COBIT: This paradigm emphasises data stewardship, which is consistent with the UK GDPR's accountability concept. COBIT also encourages continuous monitoring and improvement, which is critical for being compliant with new rules such as the UK GDPR(DPOrganizer, 2023).

1.2.3 Beyond Compliance: Building Trust and Minimizing Risks

Data Minimization: All frameworks support collecting only the information required for public health goals. This decreases the quantity of sensitive data stored, lowering privacy risks and the likelihood of a security compromise. For example, CCTV footage may be anonymised by blurring faces while maintaining location data for contact tracking (Fontes et al., 2022).

Transparency: Clear and succinct privacy notifications outlining data collecting procedures are critical to establishing public trust. All of these frameworks support the documentation of security procedures. This material can be easily modified to generate user-friendly privacy notices that everyone can comprehend (Accountability Framework, n.d.).

User Control: Individuals have the right to access, amend, or erase personal data under the UK GDPR. These frameworks support access control and data management procedures. Organisations can support user control mechanisms by implementing strong access controls and data management procedures, allowing users to manage their own data and encouraging trust in the system(ICO, 2023).

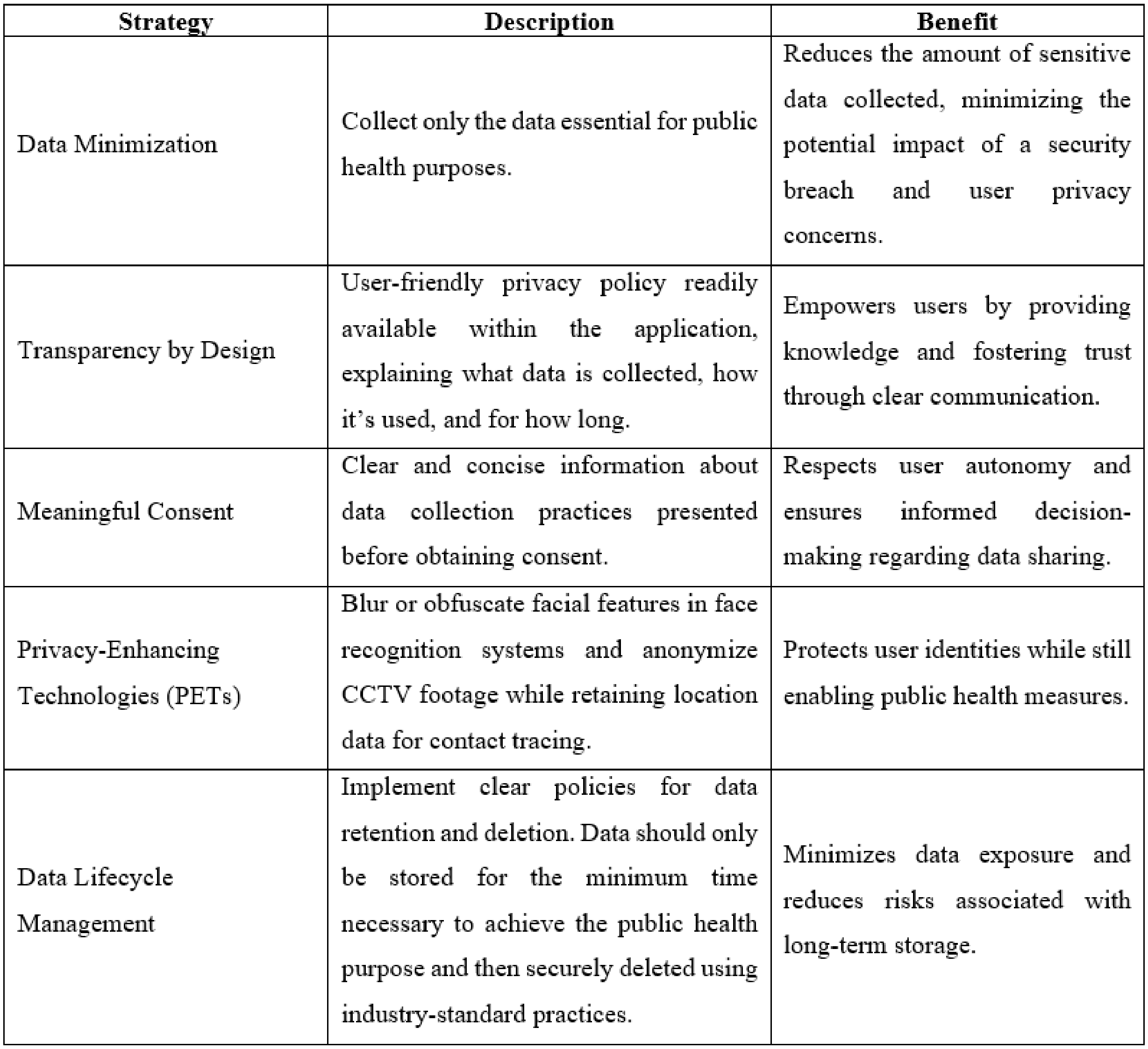
1.2.4 Putting it All Together: A Roadmap for Success

Perform a thorough risk assessment: Determine the data security and privacy concerns associated with the chosen technology (ico.org.uk, 2023).

Create a comprehensive security strategy: This strategy should include controls from all frameworks that are consistent with PbDD principles and UK GDPR standards (ico.org.uk, 2023).

Regular audits and penetration testing: Critical for discovering and fixing system vulnerabilities(ico.org.uk,2023).

User Access Controls and Data Management: Implement strong access controls and data management procedures to support user rights under the UK GDPR. Clear and concise privacy notices: Maintain clear and concise privacy statements that describe data collection procedures and user rights in plain language (ico.org.uk, 2023).



Strategy	Description	Benefit
Data Minimization	Collect only the data essential for public health purposes.	Reduces the amount of sensitive data collected, minimizing the potential impact of a security breach and user privacy concerns.
Transparency by Design	User-friendly privacy policy readily available within the application, explaining what data is collected, how it's used, and for how long.	Empowers users by providing knowledge and fostering trust through clear communication.
Meaningful Consent	Clear and concise information about data collection practices presented before obtaining consent.	Respects user autonomy and ensures informed decision-making regarding data sharing.
Privacy-Enhancing Technologies (PETs)	Blur or obfuscate facial features in face recognition systems and anonymize CCTV footage while retaining location data for contact tracing.	Protects user identities while still enabling public health measures.
Data Lifecycle Management	Implement clear policies for data retention and deletion. Data should only be stored for the minimum time necessary to achieve the public health purpose and then securely deleted using industry-standard practices.	Minimizes data exposure and reduces risks associated with long-term storage.

Figure 2 - Strategies of balancing User's privacy

1.3 Incident Response and Reporting for Implementation of Security

Developing and executing strong security measures is important for protecting CCTV or Face Recognition systems used for public health surveillance. Here is a description of the essential techniques for creating a secure environment and efficiently responding to security problems.

1.3.1 Access Controls

Implement rigorous access controls to prevent unauthorised access to CCTV or Face Recognition systems. This involves user authentication (multi-factor authentication is encouraged) and permission (NIST, 2021).

1.3.2 Data Security

Encrypt data both at rest and during transit. Encryption scrambles data, rendering it illegible to unauthorised users even if intercepted. Implement data categorization policies to categorise data according to its sensitivity. This helps to prioritise security measures and ensures that the most sensitive data is protected to the fullest extent possible. Backup your data on a regular basis and store it securely offsite to ensure data recovery in the event of a cyberattack or hardware failure (NIST, 2021).

1.3.3 Network Security

Set up firewalls to monitor and restrict incoming and outgoing network traffic, preventing suspicious activities. Update all software and firmware on CCTV or Face Recognition systems to fix known vulnerabilities. Segment your network to separate important and less critical components (NIST, 2021).

1.3.4 Incident Response Plan

Create a comprehensive incident response strategy that describes what procedures to follow in the case of a security problem. This strategy should outline methods for detecting, containing, eliminating, and recovering from an incident(NIST, 2021).

1.3.5 Incident Detection and Reporting

Use security monitoring tools to detect any suspicious activity on your network and systems. These technologies can help detect potential security incidents early on. Create explicit protocols for reporting security incidents. This includes a clear mechanism for employees to report suspicious activities, as well as a single point of contact for such reports (NIST, 2021).

1.3.6 Investigation and Containment

When you identify a security incident, execute your incident response strategy to determine the type and scope of the incident. To avoid additional damage, keep the crisis under control. This could include isolating compromised systems or taking other steps to restrict the attacker's access (NIST, 2021).

1.3.7 Eradication and Recovery

Eliminate the underlying cause of the occurrence to prevent it from occurring again. This could include eliminating malware, correcting vulnerabilities, or performing other appropriate activities. Create a recovery strategy to restore damaged systems and data to operational status. This involves having backups ready for a speedy restore (NIST, 2021).

1.3.8 Reporting and Post-Incident Review

Report the event to the proper authorities as mandated by law or regulation. Conduct an in-depth post-incident review to identify lessons learned and improve your security posture. This helps to prevent such occurrences from occurring in the future (NIST, 2021).

1.3.9 Additional Approaches

Penetration Testing: Perform penetration testing on a regular basis to identify holes in your CCTV or facial recognition systems. Penetration testing simulates a cyberattack to identify weaknesses that attackers may exploit(Imperva, 2019).

Vulnerability Management: Proactively discover, prioritise, and remedy vulnerabilities in your systems and applications(Imperva, 2019).

SIEM (Security Information and Event Management) systems: Set up a SIEM system to collect and analyse security logs from various sources. This allows you to discover security incidents more quickly and efficiently (Palo Alto Networks, n.d.).

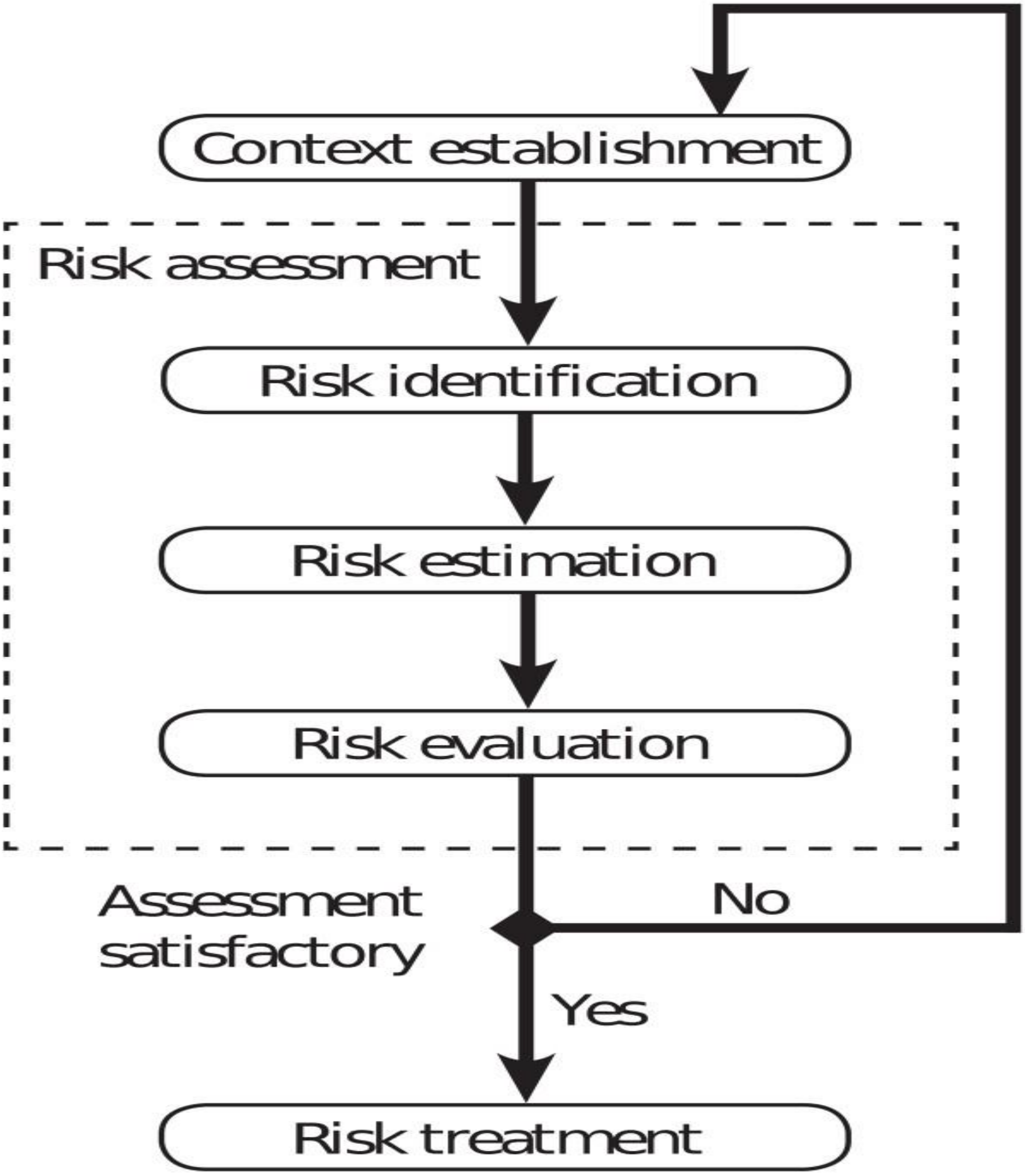


Figure 3 Workflow of Risk Assessment

Chapter - 2

2.1 MGM Grand

In September 2023, MGM Resorts, a global casino operator, experienced a cyberattack that caused several days of disruption to its operations.. Issues with digital key cards, electronic payment systems, gambling machines, ATMs, and online reservations were brought up by visitors. For certain transactions, the business was forced to use pen and paper. Affected bookings were exempt from alteration and cancellation penalties(Sanchez, 2024).

2.1.1 Description of the attack

Although the full impact of the MGM Resorts attack is still being felt, the corporation is probably going to suffer serious financial and reputational setbacks. With over 70,000 employees, MGM Resorts is one of the biggest employers in Nevada. In addition, the corporation manages resorts in Massachusetts, New Jersey, Maryland, and Michigan(Sanchez, 2024)..

Increased legal responsibility and regulatory scrutiny, decreased consumer loyalty and trust, lost revenue from disrupted operations, and higher costs for cybersecurity enhancements and remediation are all possible outcomes of the incident. The assault may potentially harm MGM's reputation and edge over competitors in the very profitable gaming and hospitality sectors(Sanchez, 2024).

2.1.2 Exposed Vulnerability

- ATMs and slot machines aren't operating or dispense money.
- Hotel rooms cannot be opened with digital key cards.
- Credit card payments not accepted by electronic payment systems.
- There are no verified online reservations accessible, and the hotel rooms' phone lines and TV service is down.
- Sportsbooks that are closed or not accepting bets.
- Some venues only accept cash.

For certain transactions, pen and paper are utilized(Sanchez, 2024)..

2.1.3 Loss to the Organization

A press release from MGM Resorts stated that the information impacted for certain of its clients who utilized MGM services prior to March 2019 included name, contact details, gender, date of birth, and driver's license number. A small percentage of clients also experienced issues with their passport number. The company's third-quarter earnings suffered $100 million loss due to the cyberattack since it had to restart certain systems and shut down others. In just two days following the attack's disclosure, MGM's stock dropped 4.1%. Tuesday, September 12, 2023 saw the stock close at $41.99, down from Friday, September 8, 2023's closing price of $43.79(Sanchez, 2024). Since then, the stock has partially recovered its losses, and on Friday, September 15, 2023, it ended $42.65.

2.2 Attackers of MGM

The MGM breach was attributed to the hacker collective known as Scattered Spider, according to TechCrunch. The ransomware group ALPHV, which has been operating since 2020 and targets big businesses with sophisticated malware that encrypts their data and demands payment for its release, is thought to include Scattered Spider as a subgroup(Sanchez, 2024)..

2.2.1 Tools used for Cyber Attack

Although Scattered Spider's actual method of hacking MGM is unknown, security researchers have some ideas based on the group's prior attacks. Ars Technica claims that Scattered Spider "phishes" for login credentials by making phone calls to staff members and help desks. After gaining access to the network with these credentials, the hackers utilise it to spread their ransomware.

Vishing, also referred to as voice phishing, is a tactic that uses social engineering and impersonation techniques to deceive gullible targets into disclosing private information. In order to make their calls appear genuine, Scattered Spider has been known to pretend to be partners, vendors, or IT personnel of the targeted company. They also utilize fake phone numbers(Sanchez, 2024).

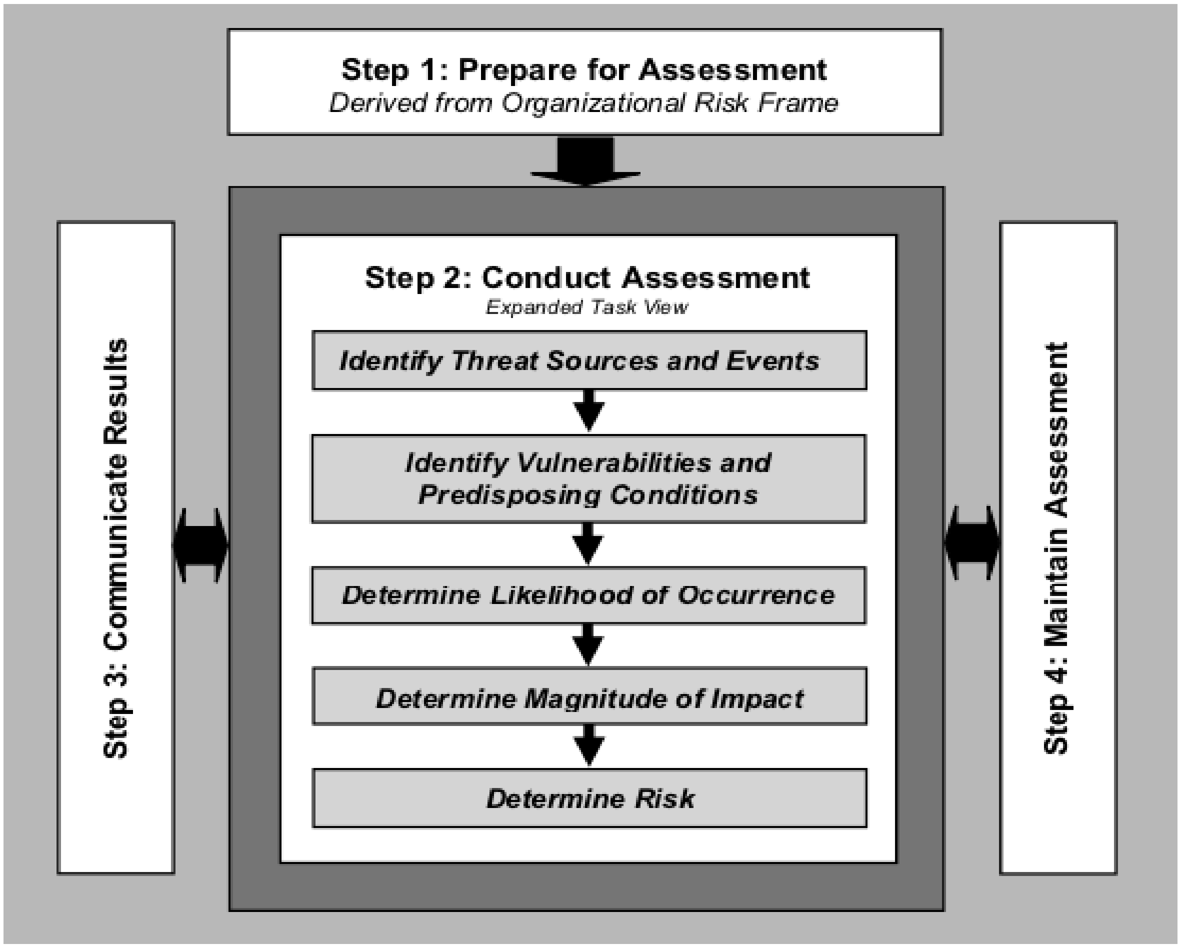

Step 1: Prepare for Assessment
Derived from Organizational Risk Frame
Step 2: Conduct Assessment
Expanded Task View
Identify Threat Sources and Events
Identify Vulnerabilities and Predisposing Conditions
Determine Likelihood of Occurrence
Determine Magnitude of Impact
Determine Risk
Step 3: Communicate Results
Step 4: Maintain Assessment

Figure 4 Flowchart of Prepare for an Assessment

2.2.2 Preventive Measures

The most important lessons learned from the MGM cyberattack are the necessity of putting in place layered cybersecurity defenses, carrying out frequent security audits and updates, creating strong incident response plans, giving employee education and awareness top priority, and successfully managing cybersecurity risks posed by third parties. Companies need strategy to cybersecurity, realizing that, given the current state of threats, depending just on one security solution is not adequate(John, 2023)..

Maintaining a proactive posture against changing threats requires regular audits and upgrades, and if a breach does occur, having a well-defined incident response plan can assist reduce its impact. Program for employee awareness and training are essential for averting human errors that might result in security incidents. Furthermore, in order to guard against supply chain vulnerabilities, it is essential to evaluate and manage third-party cybersecurity-threats (John, 2023).

Electric's Chief Information Security Officer (CISO), Aaron Shier-law, counsels' companies and IT divisions to keep upper management up to date on the latest developments and threats in cybersecurity. This emphasizes how crucial it is to keep raising awareness and advocating for cybersecurity efforts within organizations in order to secure funding and support (John, 2023).

2.3 IMPLEMENTATION OF RISK MANAGEMENT

2.3.1 Personal Identifiable Information

Any information that, by itself or related with other data, can be used to identify a specific person is referred to as personally identifiable information, or PII. This consists of:

- Name (last name plus first initial coupled with entire name)
- Gender
- Date of Birth
- Contact Details
- Driver's license number.

Known Threats

Unauthorized-Access: Data breaches can occur when hackers or other data breachers obtain access to databases or systems that hold PII.

Phishing: Cybercriminals may use phishing emails or messages to divert people and breach the PII, such as bank account details or login credentials.

Malware: Malicious software like spyware or key-loggers can take personal information from any high-end machines.

Breach of sensitive information: Unauthorized access to databases or systems holding PII can result in fraud or identity theft.

Vulnerability Description

Organizations should adopt a complete data protection strategy that includes encryption, access controls, employee training, frequent security assessments, and adherence to applicable laws and standards in order to reduce these vulnerabilities. Furthermore, in order to identify and address security problems involving PII, continuous monitoring and incident response capabilities are crucial. Since cybercriminals may use this information for fraudulent, identity-theft, and other nefarious purposes, its disclosure puts impacted parties at serious risk (imperva, 2022).

Mitigation

PII should be encrypted both while it is in transit and at rest to help prevent unwanted access to the information. The confidentiality and integrity of the data should be protected by using robust encryption techniques and key management procedures (imperva, 2022).

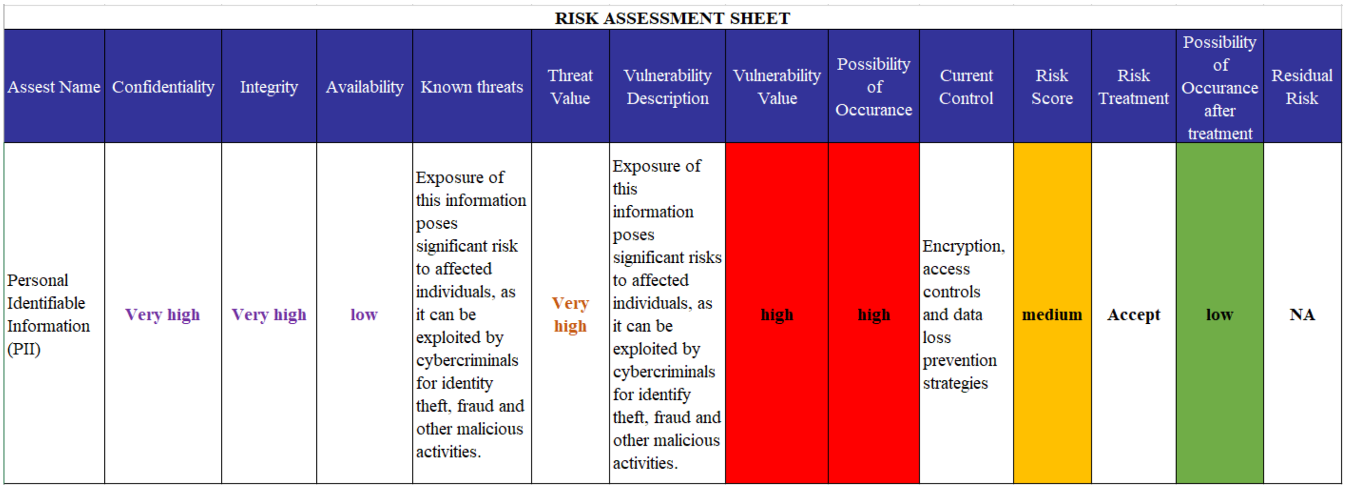
Access Controls: By putting in place access controls like multi-factor authentication (MFA), least privilege principle, and role-based access control (RBAC), only authorized workers who need it to perform their jobs are able to access PII (imperva, 2022).

Data masking: During testing, development, or training operations, the risk of exposure is decreased by masking or anonymizing PII in non-production contexts (imperva, 2022).

Data Minimization: Less sensitive data is at risk when PII is only collected, stored, and retained for as long as is required for business objectives (imperva, 2022).

Secure Transmission: By utilizing protocols like HTTPS, SSL/TLS, or VPNs to provide secure transmission of personally identifiable information over networks, data is shielded from interception and eavesdropping (imperva, 2022).

Secure Storage: Preventing unauthorized access or theft is made easier by storing PII in secure settings with sufficient logical and physical protections, intrusion detection systems (IDS), and access controls (imperva, 2022).



RISK ASSESSMENT SHEET

Assest Name	Confidentiality	Integrity	Availability	Known threats	Threat Value	Vulnerability Description	Vulnerability Value	Possibility of Occurance	Current Control	Risk Score	Risk Treatment	Possibility of Occurance after treatment	Residual Risk
Personal Identifiable Information (PII)	**Very high**	**Very high**	**low**	Exposure of this information poses significant risk to affected individuals, as it can be exploited by cybercriminals for identity theft, fraud and other malicious activities.	**Very high**	Exposure of this information poses significant risks to affected individuals, as it can be exploited by cybercriminals for identify theft, fraud and other malicious activities.	**high**	**high**	Encryption, access controls and data loss prevention strategies	**medium**	**Accept**	**low**	**NA**

Figure 5- Personal Identifiable Information (PII) – Risk Control

2.3.2 Online Card Payment

Since cybercriminals may use this information for fraudulent, identity-theft, and other purposes, it may put victims at high risk.

Known Threats

Card skimming: Devices put on payment terminals or hacked e-commerce websites have the ability to gather card information, such as security codes, expiration dates, and card numbers, which can be used fraudulently (b2b.mastercard.com, n.d.).

Man-In-The-Middle Attacks: During a payment, an attacker may intercept information going between a cardholder's device and the merchant website in order to obtain sensitive data, like login credentials or card-details (b2b.mastercard.com, n.d.).

Identity Theft: When card details from online transactions are compromised, identity thieves can use the information to start false accounts or conduct unlawful purchases by pretending to be real people(b2b.mastercard.com, n.d.).

Unauthorized Access to Payment Data: Cybercriminals may be able to obtain sensitive cardholder information through weak authentication procedures or businesses' unsafe storage of payment data (b2b.mastercard.com, n.d.).

Vulnerability Description

Data Transmission Through Insecure Channels: Payment card information can be collected by hackers using methods like network sniffing if it is communicated through insecure channels, such as unencrypted connections or weak protocols (b2b.mastercard.com, n.d.).

Weak Authentication techniques: The absence of multi-factor authentication or the use of weak passwords are examples of inadequate authentication techniques that might facilitate attackers' attempts to access user accounts without authorization and conduct fraudulent activities (b2b.mastercard.com, n.d.).

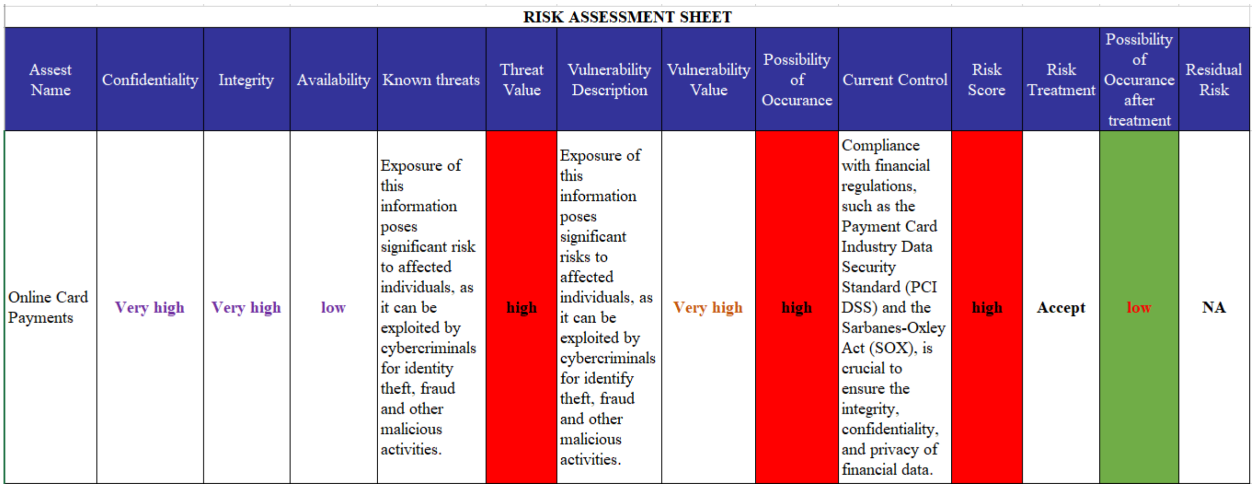
Mitigation

Encryption: To safeguard the transfer of credit card information across networks, use robust encryption techniques (b2b.mastercard.com, n.d.).

Tokenization: During payment transactions, replace sensitive cardholder data with distinct tokens. This lessens the possibility of real card numbers being exposed in merchant systems and lessens the effect of data breaches (b2b.mastercard.com, n.d.).

Secure Payment Forms: Create and update secure payment forms for mobile apps and websites. In order to guard against client-side vulnerabilities like XSS, utilise secure coding techniques and include input validation and output encoding to prevent injection attacks (b2b.mastercard.com, n.d.).

Enforce strong authentication protocols, including multi-factor authentication (MFA), to confirm users' identities when they make payments (b2b.mastercard.com, n.d.).



RISK ASSESSMENT SHEET

Assest Name	Confidentiality	Integrity	Availability	Known threats	Threat Value	Vulnerability Description	Vulnerability Value	Possibility of Occurance	Current Control	Risk Score	Risk Treatment	Possibility of Occurance after treatment	Residual Risk
Online Card Payments	Very high	Very high	low	Exposure of this information poses significant risk to affected individuals, as it can be exploited by cybercriminals for identity theft, fraud and other malicious activities.	high	Exposure of this information poses significant risks to affected individuals, as it can be exploited by cybercriminals for identify theft, fraud and other malicious activities.	Very high	high	Compliance with financial regulations, such as the Payment Card Industry Data Security Standard (PCI DSS) and the Sarbanes-Oxley Act (SOX), is crucial to ensure the integrity, confidentiality, and privacy of financial data.	high	Accept	low	NA

Figure 6 Online Card Payments – Risk Control

2.3.3 Digital Key Cards

Unauthorized Access: Hackers may intercept, copy, or modify digital card keys if they are not properly secured, giving them access to locked places or cars without authorization. Attackers can attack high-end digital keys by taking advantage of defects in mobile apps, weak encryption, or unsafe transmission methods.

Vulnerability Description

Insecure Transmission: Unsecure communication routes may be used to transfer digital card keys between systems and devices. Attackers could intercept and eavesdrop on the transmission to get sensitive key information if encryption is inadequate or non-existent (owasp.org, n.d.).

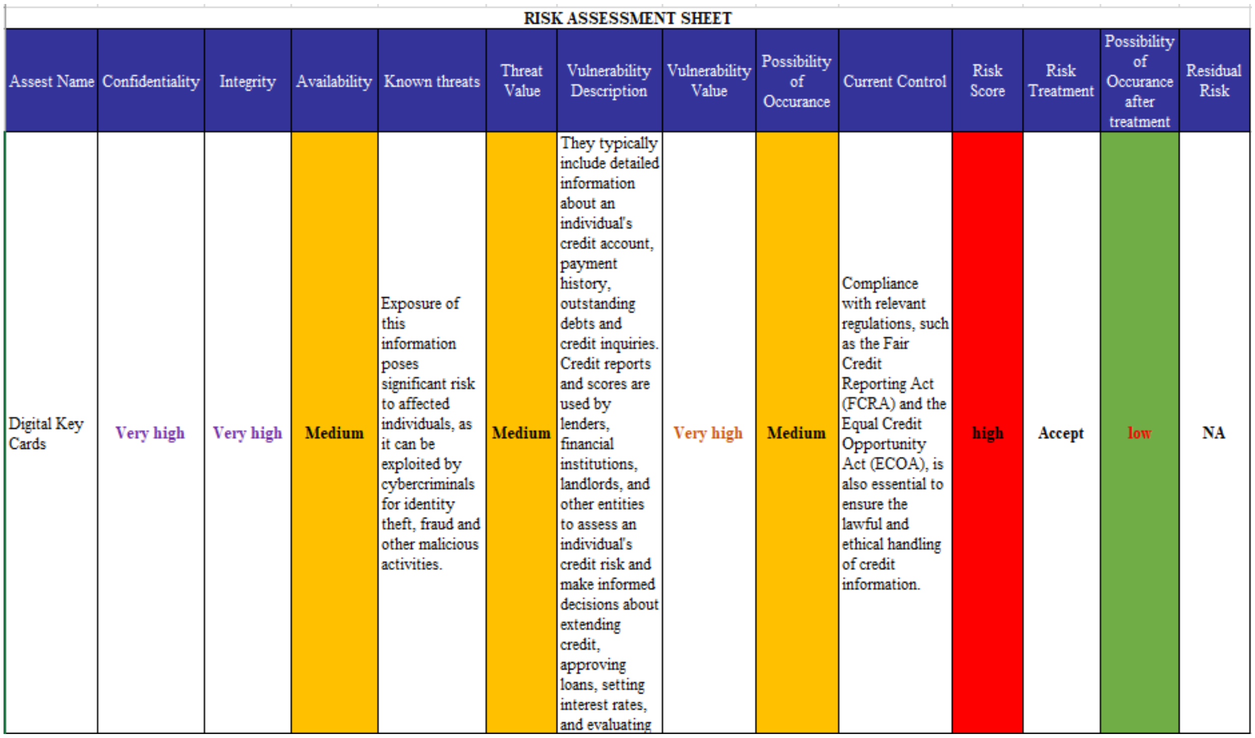
Mobile App Security: To store and maintain key credentials, a lot of digital card key systems rely on mobile applications. Attackers could compromise the keys by taking advantage of flaws in these mobile apps, such as improper data security procedures, unsafe key storage, or a lack of secure coding techniques (owasp.org, n.d.).

Mitigation

Encryption: To safeguard the transfer of credit card information across networks, use robust encryption techniques. To make sure that data transferred between clients and servers is encrypted and shielded from eavesdropping, use protocols like Transport Layer Security (TLS) (owasp.org, n.d.).

Tokenization: During payment transactions, replace sensitive cardholder data with distinct tokens. This lessens the possibility of real card numbers being exposed in merchant systems and lessens the effect of data breaches (owasp.org, n.d.).

Secure Payment Forms: Create and update secure payment forms for mobile apps and websites. In order to guard against client-side vulnerabilities like XSS, utilise secure coding techniques and include input validation and output encoding to prevent injection attacks (owasp.org, n.d.).



RISK ASSESSMENT SHEET

Assest Name	Confidentiality	Integrity	Availability	Known threats	Threat Value	Vulnerability Description	Vulnerability Value	Possibility of Occurance	Current Control	Risk Score	Risk Treatment	Possibility of Occurance after treatment	Residual Risk
Digital Key Cards	Very high	Very high	Medium	Exposure of this information poses significant risk to affected individuals, as it can be exploited by cybercriminals for identity theft, fraud and other malicious activities.	Medium	They typically include detailed information about an individual's credit account, payment history, outstanding debts and credit inquiries. Credit reports and scores are used by lenders, financial institutions, landlords, and other entities to assess an individual's credit risk and make informed decisions about extending credit, approving loans, setting interest rates, and evaluating	Very high	Medium	Compliance with relevant regulations, such as the Fair Credit Reporting Act (FCRA) and the Equal Credit Opportunity Act (ECOA), is also essential to ensure the lawful and ethical handling of credit information.	high	Accept	low	NA

Figure 7 Digital Key Cards – Risk Control

Chapter – 3

3.1 Cisco Cybersecurity Essentials – Cisco Packet Tracer

Cisco Packet Tracer offered a practical environment through which enabled me to gain wide range of experience in configuration, security, troubleshooting-network devices and protocols.

Network Design and Configuration: In this phase I studied the complex network topologies that includes routers, switches, firewalls and devices (www.linkedin.com, n.d.).

Security Protocols and Mechanisms: In this phase I studied briefly about the Access Control List, VPN and Secure Shell as well (www.linkedin.com, n.d.).

Intrusion Detection and Prevention: In this module, I learnt much about the IDPS rules which is used to detect and respond to suspicious activities likely as port scans (www.linkedin.com, n.d.).

Network Monitoring and Analysis: In this module I have used built-in-utilities as Wireshark, to identify potential security (www.linkedin.com, n.d.).

3.2 Immersive Labs

In this lab, I have learnt the cybersecurity fundamentals which is key branched to offensive and defensive security.

Cybersecurity Fundamentals: As a fresher on cybersecurity, covering vocabulary, concepts, and principles. Network security includes safeguarding network infrastructure, decrypting data, and comprehending network protocols. Techniques for identifying, handling, and minimizing cybersecurity events are known as incident response strategies (Immersive Labs, 2019).

Offensive Security: Interactive labs for identifying and taking advantage of security holes in wireless networks, web applications, and network infrastructure. Phishing assaults and pretexting are two strategies that can be practiced in simulated scenarios. Exercises are practical imitations of adversarial strategies and tactics used to evaluate the defensive capabilities of an organisation (Immersive Labs, 2019).

Defensive Security: Security operations centre training focuses on monitoring, analysing, and responding to security issues in a SOC environment. Techniques for actively searching for evidence of harmful activity within an organization's network. Incident response planning entails creating and implementing response strategies to effectively manage and mitigate cybersecurity issues (Immersive Labs, 2019).

Conclusion

The development of monitoring and contact tracing technologies provides a unique opportunity to solve public health issues. However, it is critical that this development is carried out with a deep regard for user privacy. We may strike a equity between these two vital requirements by implementing a Data Protection by Design and Default (PbDD) approach and following relevant rules such as the UK GDPR.

This assessment provides a comprehensive plan for adding PbDD principles into the project. This includes limiting data collection, guaranteeing user control through meaningful consent and access procedures, emphasising openness, and implementing strong security measures. Furthermore, complying with the UK GDPR assures legal compliance and increases user trust.

The Risk assessment is based on all these above mentioned factors which are highly correlated with the docile of rule and hence it is formed on basis of the UK GDPR which helps to analyse any cyberattack and it’s upcoming issues has being explained.

References

1. Accountability Framework. (n.d.). Available at: https://ico.org.uk/media/for-organisations/accountability-framework-0-0.pdf.

2. A.5 INFORMATION SECURITY POLICIES A.5.1 Management direction of information security A.5.1.1 Policies for Information Security - A.5.1.2 Review of the policies for information security - ISO 27001 CONTROLS A.6 ORGANZATION OF INFORMATION SECURITY. (n.d.). Available at: https://www.cssia.org/wp-content/uploads/2020/01/ISO_27001_Standard.pdf.

3. b2b.mastercard.com. (n.d.). *What is skimming in cybersecurity?* [online] Available at:https://b2b.mastercard.com/news-and-insights/blog/what-is-skimming-in-cybersecurity/.

4. DPOrganizer. (2023). *The Role of Accountability in GDPR: Leveraging ICO's Framework for Effective Compliance*. [online] Available at: https://www.dporganizer.com/blog/the-role-of-accountability-in-gdpr-leveraging-icos-framework-for-effective-compliance/ [Accessed 8 May 2024].

5. Fontes, C., Hohma, E., Corrigan, C.C. and Lütge, C. (2022). AI-powered public surveillance systems: why we (might) need them and how we want them. *Technology in Society*, [online] 71(0160-791X), p.102137. doi:https://doi.org/10.1016/j.techsoc.2022.102137.

6. ICO (2018). Essential Guide to the General Data Protection Regulation (GDPR). *Guide to the General Data Protection Regulation (GDPR)*. [online] doi: ICO (2023). *Data protection by design and default*. [online] ico.org.uk. Available at: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/guide-to-accountability-and-governance/accountability-and-governance/data-protection-by-design-and-default/.

7. ico.org.uk. (2023). *Risks and data protection impact assessments (DPIAs)*. [online] Available at: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/accountability-framework/risks-and-data-protection-impact-assessments-dpias/.

8. Immersive Labs. (2019). *Immersive Labs*. [online] Available at: https://www.immersivelabs.com/.

9. Imperva (2019). *What is Penetration Testing | Step-By-Step Process & Methods | Imperva*. [online] Imperva. Available at: https://www.imperva.com/learn/application-security/penetration-testing/.

10. imperva (2022). *What is Data Security | Threats, Risks & Solutions | Imperva*. [online] Learning Center. Available at: https://www.imperva.com/learn/data-security/data-security/.

11. Information Commissioner's Office (2012). *Anonymisation: managing data protection risk code of practice*. [online] Available at: https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf.

12. Irwin, L. (2021). *IT Governance Blog: the 5 Controls of the Cyber Essentials Scheme*. [online] IT Governance UK Blog. Available at: https://www.itgovernance.co.uk/blog/essential-security-cyber-essentials-and-its-five-controls.

13. John, M. (2023). *MGM Cyber Attack: Cybersecurity Lessons Learned for Businesses*. [online] Electric. Available at: https://www.electric.ai/blog/mgm-cyber-attack-cybersecurity-lessons-learned-for-businesses.

14. NIST (2021). Security and Privacy Controls for Federal Information Systems and Organizations. *NIST*. [online] doi:https://doi.org/10.6028/nist.sp.800-53r4.

15. owasp.org. (n.d.). *M3: Insecure Communication | OWASP*. [online] Available at: https://owasp.org/www-project-mobile-top-10/2016-risks/m3-insecure-communication.

16. Palo Alto Networks. (n.d.). *What Is Security Information and Event Management (SIEM)?* [online] Available at: https://www.paloaltonetworks.co.uk/cyberpedia/what-is-security-information-and-event-management-SIEM#:~:text=SIEM%20works%20by%20collecting%20security[Accessed 8 May 2024].

17. Sanchez, D. (2024). *The 2023 Cyberattack on the MGM Resort Explained*. [online] Inszone Insurance. Available at: https://inszoneinsurance.com/blog/cyberattack-mgm-resort-explained#:~:text=The%20stolen%20data%20included%20names.

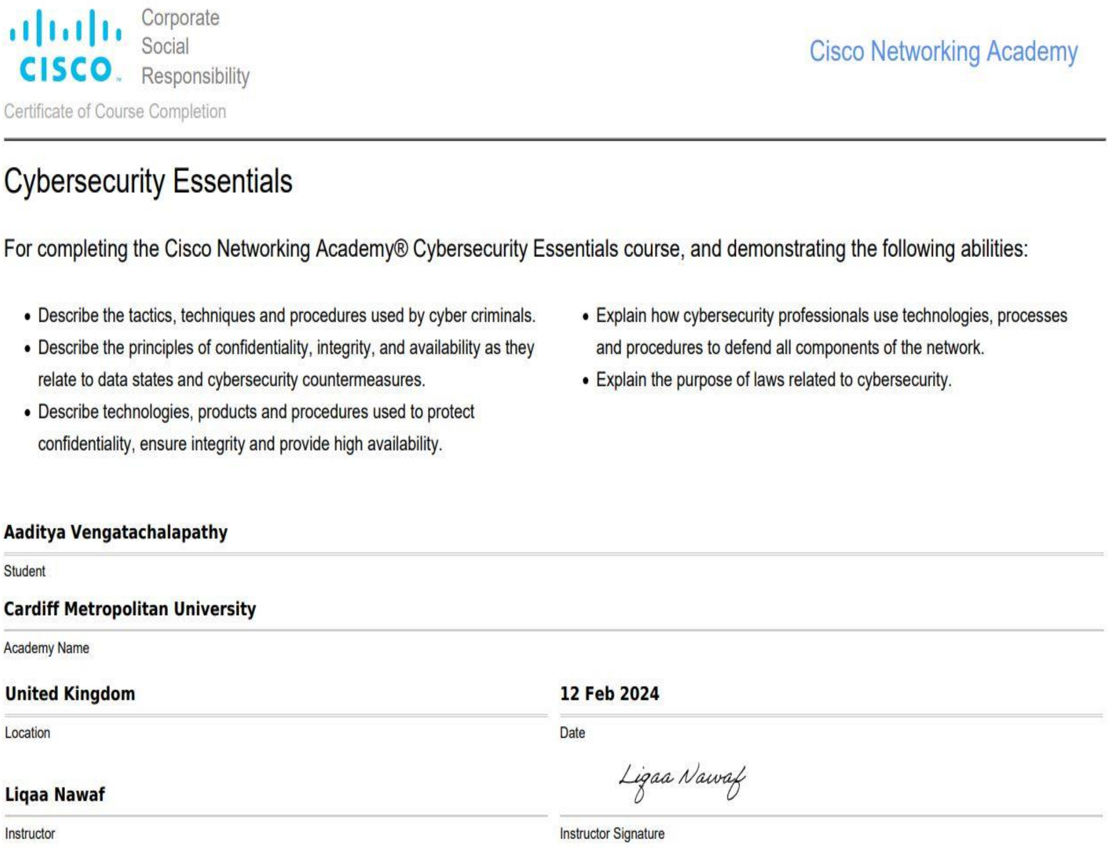
18. www.linkedin.com. (n.d.). *Exploring Cisco Packet Tracer: A Comprehensive Guide to Network Simulation*. [online] Available at: https://www.linkedin.com/pulse/exploring-cisco-packet-tracer-comprehensive-guide-network-suresh-d8skc/[Accessed 8 May 2024].

19. www.ncsc.gov.uk. (2022). *Reducing data exfiltration by malicious insiders*. [online] Available at: https://www.ncsc.gov.uk/guidance/reducing-data-exfiltration-by-malicious-insiders.

20. www.onetrust.com. (n.d.). *EU-US Data Privacy Framework resource kit*. [online] Available at: [Accessed 8 May 2024].https://www.onetrust.com/resources/eu-us-data-privacy-framework-resource-kit/?gclid=Cj0KCQjwxeyxBhC7ARIsAC7dS3-AFj1bxFPZOsOz0xSa5iw0bg9pKhUOoH7hbi8n23Q26v6RtdDMI-8aAnMsEALw_wcB&ef_id=Cj0KCQjwxeyxBhC7ARIsAC7dS3-AFj1bxFPZOsOz0xSa5iw0bg9pKhUOoH7hbi8n23Q26v6RtdDMI-8aAnMsEALw_wcB:G:s&s_kwcid=AL

Appendices

A1. CISCO – Cybersecurity Essentials



CISCO Corporate Social Responsibility

Certificate of Course Completion

Cisco Networking Academy

Cybersecurity Essentials

For completing the Cisco Networking Academy® Cybersecurity Essentials course, and demonstrating the following abilities:

- Describe the tactics, techniques and procedures used by cyber criminals.
- Describe the principles of confidentiality, integrity, and availability as they relate to data states and cybersecurity countermeasures.
- Describe technologies, products and procedures used to protect confidentiality, ensure integrity and provide high availability.
- Explain how cybersecurity professionals use technologies, processes and procedures to defend all components of the network.
- Explain the purpose of laws related to cybersecurity.

Aaditya Vengatachalapathy

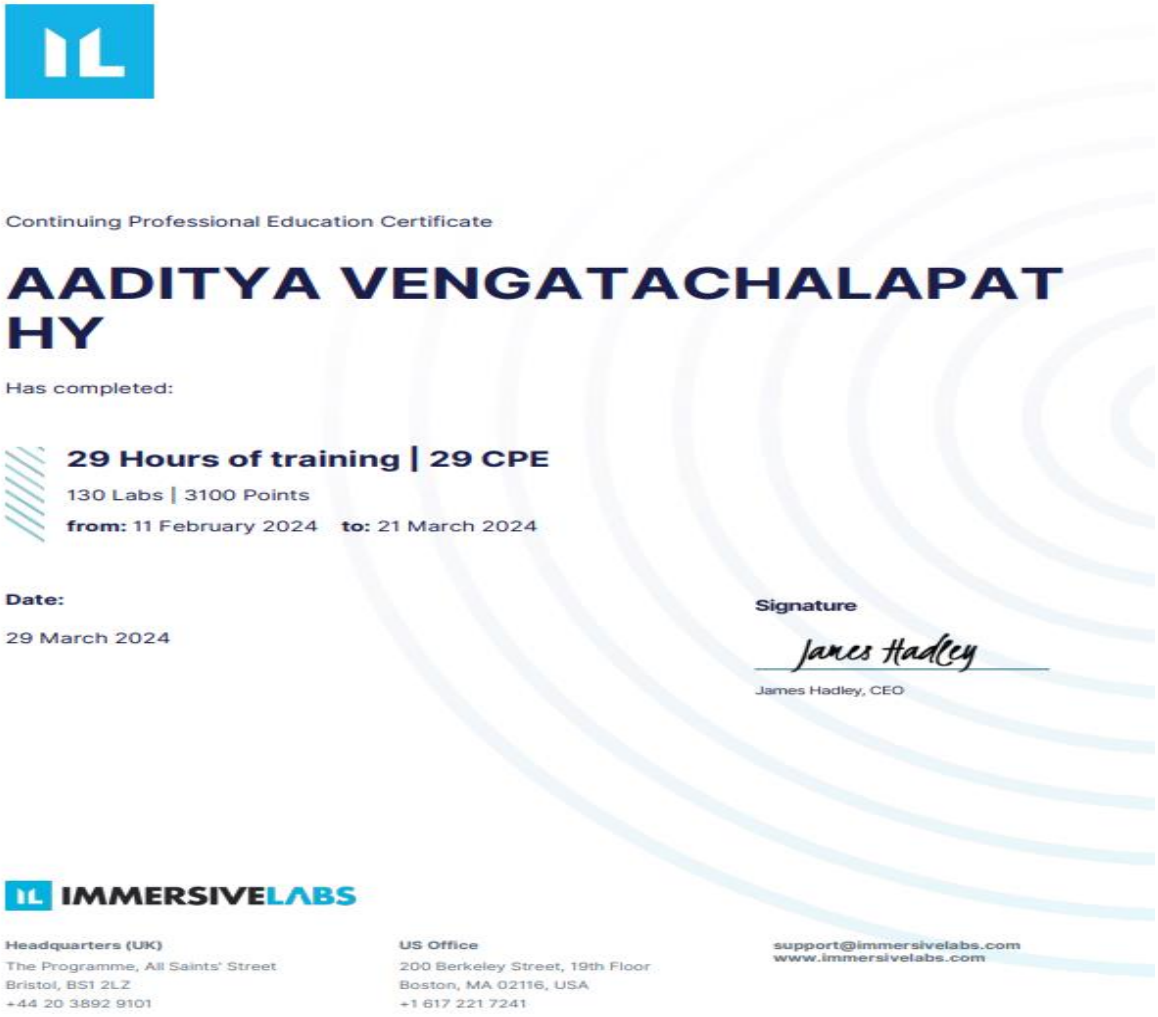
Student

Cardiff Metropolitan University

Academy Name

United Kingdom	**12 Feb 2024**
Location	Date
Liqaa Nawaf	Liqaa Nawaf
Instructor	Instructor Signature

A2. Immersive Labs



Continuing Professional Education Certificate

AADITYA VENGATACHALAPATHY

Has completed:

29 Hours of training | 29 CPE

130 Labs | 3100 Points

from: 11 February 2024 **to:** 21 March 2024

Date:

29 March 2024

Signature

James Hadley

James Hadley, CEO

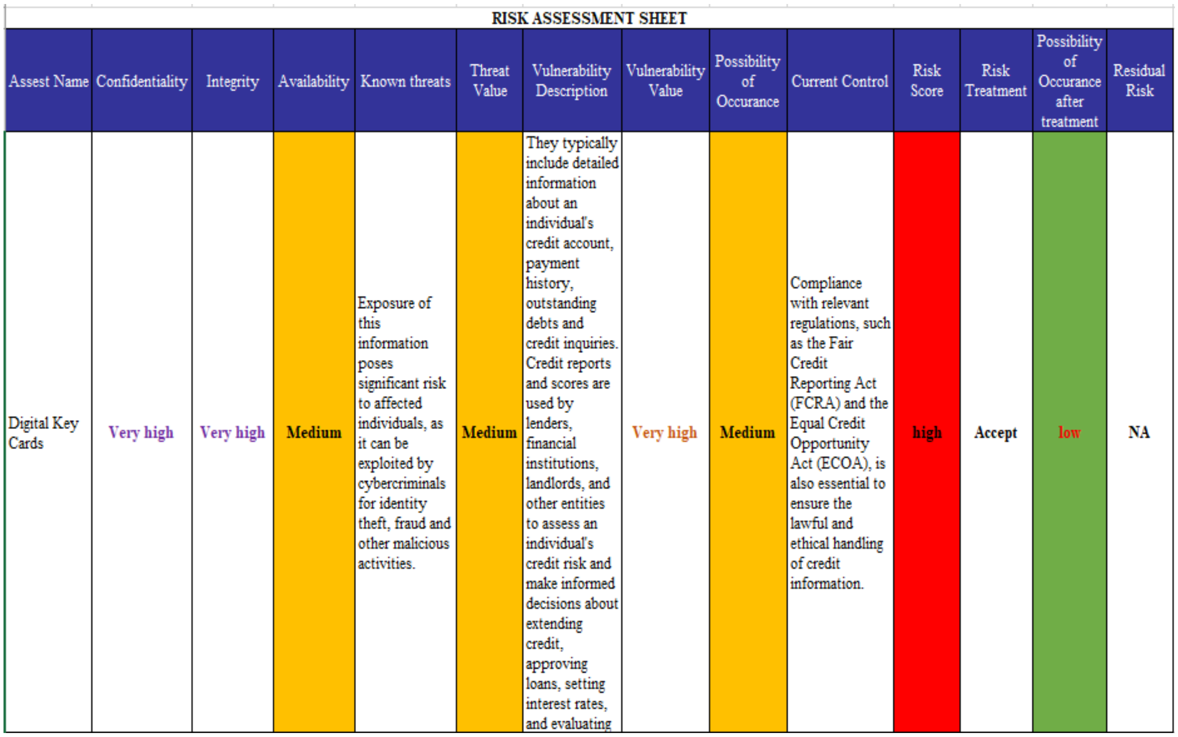
IMMERSIVELABS

Headquarters (UK)
The Programme, All Saints' Street
Bristol, BS1 2LZ
+44 20 3892 9101

US Office
200 Berkeley Street, 19th Floor
Boston, MA 02116, USA
+1 617 221 7241

support@immersivelabs.com
www.immersivelabs.com

A3. Risk Assessment – Microsoft Excel



RISK ASSESSMENT SHEET

Assest Name	Confidentiality	Integrity	Availability	Known threats	Threat Value	Vulnerability Description	Vulnerability Value	Possibility of Occurance	Current Control	Risk Score	Risk Treatment	Possibility of Occurance after treatment	Residual Risk
Digital Key Cards	Very high	Very high	Medium	Exposure of this information poses significant risk to affected individuals, as it can be exploited by cybercriminals for identity theft, fraud and other malicious activities.	Medium	They typically include detailed information about an individual's credit account, payment history, outstanding debts and credit inquiries. Credit reports and scores are used by lenders, financial institutions, landlords, and other entities to assess an individual's credit risk and make informed decisions about extending credit, approving loans, setting interest rates, and evaluating	Very high	Medium	Compliance with relevant regulations, such as the Fair Credit Reporting Act (FCRA) and the Equal Credit Opportunity Act (ECOA), is also essential to ensure the lawful and ethical handling of credit information.	high	Accept	low	NA