# Cybersecurity Risk Assessment

Drafted by Oyindamola Olayiwola

15th October, 2024

# Executive Summary

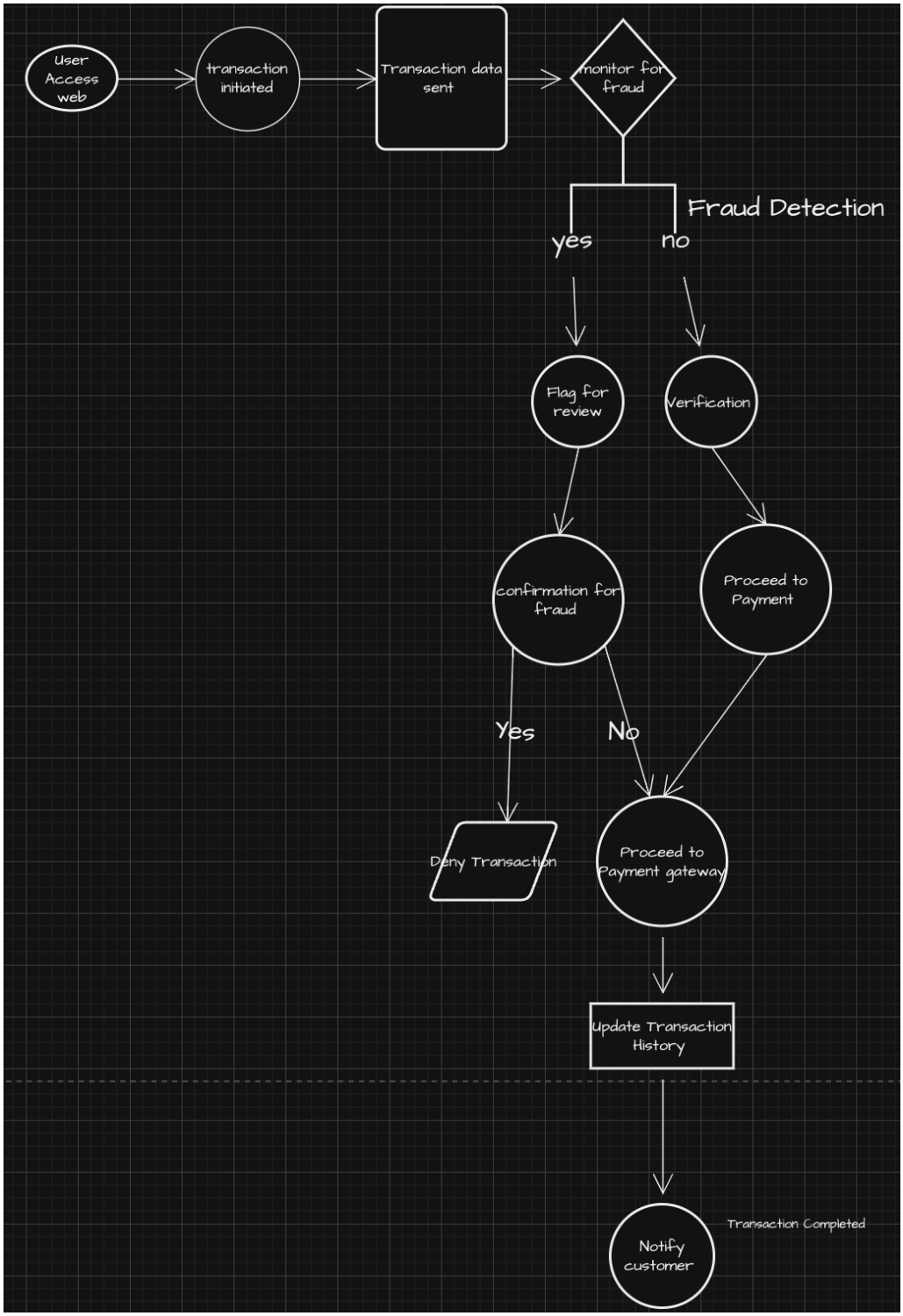
This risk assessment report evaluates the critical cybersecurity risks associated with the acquisition of Garden City Wealth Management by Jones & Davis. The assessment highlights key vulnerabilities, including potential data breaches, credential theft, unauthorized access to sensitive investment portfolio data, encryption key theft, and non-compliance with data protection regulations.

Among the highest-impact risks identified are:

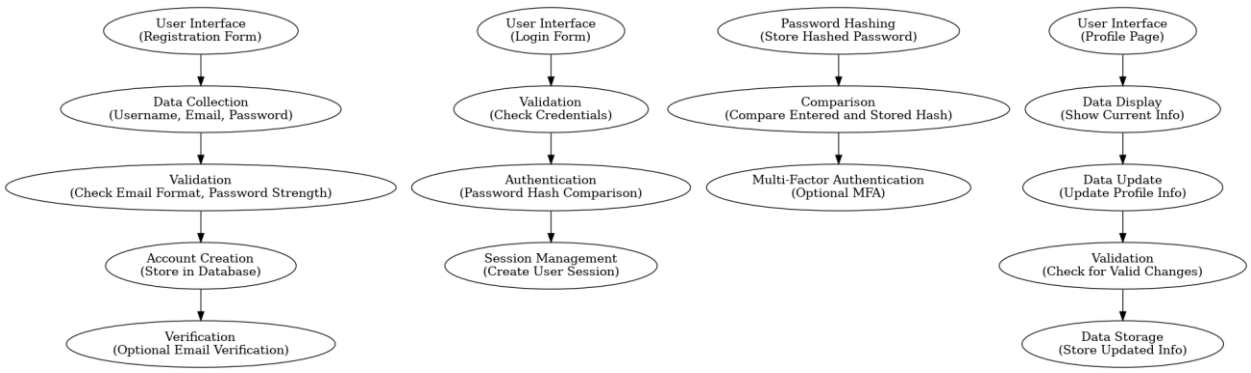
- Data Breach: Exposing customer personal and financial information could lead to significant financial losses, regulatory fines, and reputational damage.
- Credential Theft: Weak passwords or stolen credentials could result in unauthorized access to critical systems, exposing customer data and enabling fraudulent activities.
- Unauthorized Access to Investment Portfolios: Weak authentication controls may allow attackers to manipulate customer portfolios, causing substantial financial harm.
- Encryption Key Theft: The compromise of encryption keys could expose sensitive data, leading to unauthorized access and decryption of confidential information.
- Non-Compliance with Data Protection Regulations: Failure to align with GDPR, CCPA, and other data protection standards may result in heavy penalties and legal repercussions.

To mitigate these risks, the report recommends strengthening encryption, enforcing multi-factor authentication, implementing regular security audits, improving employee training on cybersecurity, and using compliance automation tools. By addressing these vulnerabilities proactively, Jones & Davis can ensure the secure integration of Garden City Wealth Management, maintain regulatory compliance, and protect sensitive customer data.

End-to-End Process Flow for Customer Account Management and Transaction Handling




Transaction Processes Flowchart



Customer Account Management Flowchart

1. Customer Account Management:

Account Creation

- User Interface: The user interacts with a registration form or interface.
- Data Collection: The user provides essential information like username, email, password, and possibly additional details.
- Validation: The system checks if the provided data is valid (e.g., email format, password strength).
- Account Creation: If validation passes, a new user account is created in the system's database.
- Verification: An email verification link or code might be sent to the user to confirm their account.

Login

- User Interface: The user enters their username or email and password.
- Validation: The system verifies the provided credentials against the stored data.
- Authentication: If credentials match, the user is authenticated and granted access to the system.
- Session Management: A session is created to track the user's activity.

Authentication

- Password Hashing: Passwords are stored as hashed values to protect against unauthorized access.
- Comparison: When a user logs in, the entered password is hashed and compared to the stored hash.
- Multi-Factor Authentication (MFA): For added security, MFA might require additional verification steps like SMS codes or security tokens.

Profile Management

- User Interface: The user accesses a profile page or settings area.
- Data Display: The system displays the user's current profile information.
- Data Update: The user can modify their profile details (e.g., name, address, preferences).
- Validation: The system validates any changes to ensure data integrity.
- Data Storage: Updated profile information is saved to the database.

People, Processes, and Technology:
People: Customers, support team, IT administrators, Developers, Database administrator.
Processes: Account creation, login and authentication, password recovery Profile Management.
Technology: Authentication servers, encryption protocols, databases for storing account data, Password Hashing Algorithms, Application
- Asset List: user credentials, authentication servers, encryption keys, user data, Databases, Application Code, Applications, Data Backup Systems etc.

2. Transaction Processes

User Interface: The customer accesses the transaction feature through a mobile or web application.

1. Transaction Initiation
    - The customer selects the type of transaction (e.g., fund transfer, purchase).
    - The user inputs transaction details, including the amount and recipient (if applicable).
2. Payment Method Selection: The user selects a payment method (e.g., credit/debit card, bank account, digital wallet).
3. Data Validation: The system verifies that the transaction details are complete and valid (e.g., sufficient funds, correct account information).
4. Fraud Detection

    System Action:

        The system analyzes the transaction against established fraud detection rules to identify any suspicious activity.

        If fraud is suspected, the transaction may be flagged for further review.

5. Transaction Processing

    System Action:

    - The system communicates with payment gateways or financial institutions to process the transaction.

    - This may involve secure transmission of payment information and authorization requests.
6. Transaction Confirmation

   System Action:

    - Upon successful processing, the system generates a confirmation message for the customer.
    - This message includes transaction details such as transaction ID, amount, and date/time.
7. Logging and Record Keeping

   System Action:

    - The transaction details are securely logged in the system for auditing and compliance purposes.
    - Relevant data is stored in the transaction database for future reference.
8. Customer Notification

   System Action:

    - The customer receives a notification (via email or app notification) confirming the transaction was successful.
    - If applicable, the customer is informed of any fees associated with the transaction.

People, Processes, and Technology:
People: Customers, payment processing team, financial institution Fraud Analyst, IT Administrator, Compliance oFFICER.
Processes: Transaction initiation, Data Validation, Transaction Procesing, and confirmation, fraud Detection, Transaction Confirmation, Customer Notification, Logging .
Technology: Payment gateways, encryption tools, fraud detection systems, secure storage for transaction logs.
processing and confirmation.

Asset List: Transaction Databaste, Application Server , Applications , Fraud Detection Systems, payment information, transaction logs, payment gateway infrastructure, encryption tools, etc.

Asset List and Risk Register

| Asset ID | Asset Name | Risk ID | Risk Description | Category | Likelihood | Impact | Risk Score | Mitigation Strategy | Owner | Status | Residual risk | Current Controls |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A00001 | Customer Data | R0001 | Data breach exposing customer personal and financial information | Security | High | Medium | High | MFA, IDS, Access Controls, Encryption | IT Security Team | In Progress | Low | Data is encrypted both in transit and at rest using AES-256. |
| A00002 | Authentication System | R0002 | Credential theft or weak password leading to unauthorized access | Security | High | High | High | Strong Password practice , MFA, Stong encryption algorithm and Hashing | IT Security Team | In Progress | Low | Multi-Factor Authentication (MFA) is enforced for all users. |
| A00003 | Transaction Ledger | R0003 | Corruption or tampering with transaction data | Data Integrity | High | Low | Medium | Access Control, Data Encrption, Data Integrity Checks, Immutable Data storage, | Wealth Management Team | In Progress | Low | Transaction logs are protected by cryptographic integrity checks. |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | Regular Backup | | | | |
| A00004 | Wealth Portfolio Data | R0004 | Unauthorized access to investment portfolio data | Security | High | Medium | High | Data Loss Prevention (DLP), MFA, IDS, Access Controls, Encryption | IT Operations Team | In Progress | Low | Role-based access control (RBAC) restricts access to sensitive data based on user roles. |
| A00005 | Payment Processing System | R0005 | Payment processing failure or delay leading to transaction issues | Operational | Medium | Medium | Medium | Choose a Reliable Payment Processor, Test and Validate Payments, implement Redundancy and Backup Plans, Monitor and Address Issues Proactively | IT Security Team | In Progress | Low | Failover payment gateways are in place. |
| A00006 | Encryption Mechanism | R0006 | Encryption key theft or failure exposing sensitive data | Security | High | High | High | Strong Key Management Practices (i.e. Regular Key Rotation, Key Separation, | | In Progress | Low | Encryption keys are stored and managed using Hardware Security Modules (HSM). |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | Key Hierarchies for different levels of data, Key backup), MFA,DLP, Encryption audits. | | | | |
| A00007 | Cloud Infrastructure | R0007 | Cloud service outage or misconfiguration | Operational | low | High | Medium | Regular disaster recovery tests, cloud configuration reviews | Cloud Operations Team | In Progress | | Cloud services have multi-region redundancy for high availability. |
| A00008 | Data migration & Backup System | R0008 | Data loss due to failure of backup systems | Operational/Data Integrity | low | low | low | Regular backup recovery testing, off-site backup replication | IT/Backup Team | In Progress | Low | Automatic daily backups are stored both on-premises and in the cloud. |
| A00009 | Fraud Detection System | R0009 | Fraud detection system failure leading to undetected fraudulent activity | Security | High | medium | High | Redundancy and Fault Tolerance, Regular Testing and Maintenance, Real-time monitoring | Security, Finance Team | In Progress | Low | Fraud detection is integrated with machine learning models to identify anomalies. |
| A00010 | Business Intelligence | R0010 | Leakage of internal | Data Integrit | Medium | low | low | DLP, restrict | Business | In Progre | Low | Access control and encryption |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Tools | | business intelligence data | y/Operational | | | | access to sensitive reports, log and monitor all access to BI data | Analytics Team | ss | | are applied to BI reports. |
| A00011 | Regulatory Compliance Data | R0011 | Non-compliance with data protection regulations | Compliance | High | Medium | High | Implement compliance automation tools, regular employee training on data handling regulations | Legal/Compliance Team | In Progress | Low | Regular compliance audits are conducted, and data processing activities are logged. |
| A00012 | Wealth Management Platform | R0012 | Unauthorized access to investment portfolios, leading to potential fraud or misuse of customer data. | Security | High | Medium | High | Strong Authentication , Implement Strong Password Policies, log and monitor activities | IT Security Team | In Progress | Low | Role-based access controls (RBAC) |
| A00013 | Customer Support and Recovery System | R0013 | Delays in account recovery processes could result in customer | operational | Medium | Medium | Medium | Streamline recovery processes, improve staff training, and | IT Operations Team | In Progress | Low | Automated ticketing system for tracking customer requests. |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | dissatisfaction and potential loss of business | | | | | enhance system uptime. | | | | |
| A00014 | Banking Infrastructure | R0014 | System outages or failures could disrupt services, leading to financial losses and negative customer experiences. | operational | High | Low | Medium | Regular stress testing, monitoring system performance, and incident response plans. | Customer Support Team | In Progress | Low | Failover systems for critical banking services are established. |

**Critical Risk Analysis: High-Impact Vulnerabilities Identified**

Both companies have undergone a thorough assessment to identify risks that may be inherent in the acquisition process and to evaluate how these risks could impact the organization. Below are the highly impacted risks that have been identified, along with their nature and recommendations for minimizing or eliminating these risks:

Risk ID:R0001
Risk Description: Data breach exposing customer personal and financial information
Nature of Risk: The exposure or theft of sensitive data, such as personally identifiable information (PII), account details, and transaction histories, can lead to significant consequences for the organization. These consequences include financial losses from remediation efforts, legal fees, or regulatory fines; reputational damage, which can result in the loss of customer trust and business opportunities; and operational disruptions, as systems may need to be shut down temporarily to address the breach.
This risk can arise from multiple sources. External cyberattacks, such as hacking or ransomware, pose a constant threat to data security. Insider threats, such as disgruntled employees or contractors with malicious intent, may also exploit system vulnerabilities. Furthermore, third-party service providers may fail to adequately secure their systems, creating additional exposure points that could lead to unauthorized access to sensitive data.
Impact:High
Likelihood: medium

Risk ID:R0002
Risk Description: Credential theft or weak password leading to unauthorized access
Nature of Risk: Credential theft or the use of weak passwords can result in unauthorized access to sensitive systems, customer accounts, and critical data. This type of risk can lead to severe consequences, such as data breaches, unauthorized transactions, and the exposure of sensitive customer and financial information. The misuse of stolen credentials can allow attackers to access privileged areas of the system, execute fraudulent activities, or even disrupt operations. This risk originates from multiple potential sources. Credential theft can occur through phishing attacks, malware infections, or brute force attempts to crack weak passwords. Insider threats also pose a risk if employees misuse their access privileges or fail to adhere to security best practices, such as password complexity requirements. Additionally, if employees or customers reuse passwords across multiple platforms, the compromise of credentials on an unrelated site could lead to unauthorized access to the banking or wealth management systems.
Impact:High
Likelihood: high

Risk ID:R0004
Risk Description: Unauthorized access to investment portfolio data
Nature of Risk: Unauthorized access to investment portfolio data poses a significant threat to customer information and financial assets. If attackers gain access, they could commit fraudulent activities like unauthorized trading, leading to substantial financial losses and reputational damage as customers lose trust in the organization. This risk can arise from weak authentication methods, such as insufficient multi-factor authentication (MFA) or lax password policies. Insider threats from employees misusing their access, as well as system vulnerabilities like outdated software or inadequate access controls, can further exacerbate the issue. Unauthorized access increases the risk of data breaches and fraud, potentially resulting in legal repercussions and customer attrition if sensitive data is compromised.
Impact: High
Likelihood: Medium

Risk ID:R0006
Risk Description: Encryption key theft or failure exposing sensitive data
Nature of Risk: The theft or failure of encryption keys can expose sensitive customer and financial information, including PII, financial records, and transaction histories. If encryption keys are compromised, the data becomes vulnerable to unauthorized access and decryption. This risk may arise from external attacks on encryption key management systems, insufficient security measures for key storage, or insider threats. Weak encryption algorithms or outdated key management practices can also result in key failure, leaving data unprotected.
Impact: High
Likelihood: Medium

Risk ID:R0011
Risk Description: Non-compliance with data protection regulations
Nature of Risk: Non-compliance with data protection regulations, such as GDPR, CCPA, or PCI DSS, can result in severe financial penalties, legal actions, and reputational damage. This risk arises from inadequate security measures, poor data management, or failure to report breaches. During the acquisition of Garden City Wealth Management by Jones & Davis, the complexity of merging systems may create compliance gaps if data protection practices are not properly aligned.
Impact:High
Likelihood: medium

Risk ID:R0012
Risk Description: Unauthorized access to investment portfolios, leading to potential fraud or misuse of customer data.
Nature of Risk: Unauthorized access to investment portfolios poses a serious threat to customer data security and financial integrity. It can lead to fraudulent activities, such as unauthorized trading, fund transfers, and exposure of sensitive information, resulting in severe financial and reputational damage to both customers and the organization. This risk may arise from weak authentication mechanisms, such as poorly designed passwords or insufficient multi-factor authentication (MFA), as well as insider threats where employees misuse access privileges. Additionally, vulnerabilities in system architecture, such as outdated software or inadequate access controls, can contribute to unauthorized access. The interdependencies of this risk include an increased likelihood of data breaches and regulatory penalties if sensitive information is compromised, potentially eroding customer trust and leading to attrition.
Impact:High
Likelihood: Medium

Risk ID:R0008
Risk Description: Fraud detection system failure leading to undetected fraudulent activity
Nature of Risk:A failure in the fraud detection system significantly threatens the organization's ability to identify and prevent fraudulent activities. If the system cannot accurately detect suspicious transactions, it may lead to substantial financial losses, unauthorized transactions, and compromised customer accounts, ultimately damaging the organization's reputation and eroding customer trust. This risk can arise from outdated algorithms, insufficient training data, or system outages that prevent effective monitoring. Additionally, false negatives may occur, where fraudulent activities go undetected. The interdependencies include increased customer complaints and potential legal consequences if fraud is not promptly identified, which can result in customer attrition.
Impact:High
Likelihood: Medium

## Mitigation Strategies for Identified Risks

Risk ID: R0001 - Data Breach

- Strong Encryption: Implement robust encryption algorithms (e.g., AES-256) to protect data both at rest and in transit.
- Regular Security Audits: Conduct regular security audits to identify vulnerabilities and address them promptly.
- Employee Training: Provide comprehensive cybersecurity training to employees to raise awareness and prevent human errors.
- Access Controls: Implement granular access controls to limit access to sensitive data based on user roles and permissions.
- Incident Response Plan: Develop and regularly test a comprehensive incident response plan to effectively handle data breaches.
- Third-Party Vendor Management: Conduct due diligence on third-party vendors and ensure they have adequate security measures in place.

Risk ID: R0002 - Credential Theft

- Multi-Factor Authentication (MFA): Require MFA for all user logins to add an extra layer of security.
- Password Policies: Enforce strong password policies, including complexity requirements and regular password changes.
- Phishing Awareness Training: Educate employees on how to recognize and avoid phishing attempts.
- Password Management Tools: Encourage employees to use password management tools to securely store and manage their credentials.
- Regular Password Audits: Conduct regular password audits to identify weak or compromised passwords.

Risk ID: R0004 - Unauthorized Access to Investment Portfolio Data

- Role-Based Access Controls (RBAC): Implement RBAC to grant access to data only on a need-to-know basis.
- Activity Monitoring: Continuously monitor user activity for suspicious patterns or unauthorized access attempts.
- Data Loss Prevention (DLP): Deploy DLP solutions to prevent unauthorized data transfers and exfiltration.
- Regular Security Patching: Keep systems and software up-to-date with the latest security patches.
- Access Reviews: Regularly review user access privileges and revoke unnecessary permissions.

Risk ID: R0006 - Encryption Key Theft

- Hardware Security Modules (HSMs): Store encryption keys in secure HSMs to protect them from unauthorized access.
- Key Rotation: Regularly rotate encryption keys to minimize the exposure of any compromised key.
- Key Separation: Implement key separation practices to prevent a single point of failure.
- Key Backup: Maintain secure backups of encryption keys to facilitate recovery in case of loss or damage.

Risk ID: R0011 - Non-Compliance with Data Protection Regulations

- Compliance Automation Tools: Utilize compliance automation tools to streamline compliance efforts and ensure adherence to regulations.
- Employee Training: Provide regular training to employees on data protection regulations and best practices.
- Data Mapping and Classification: Conduct thorough data mapping and classification to understand the sensitivity of data and apply appropriate controls.
- Compliance Audits: Conduct regular compliance audits to identify and address any gaps or non-compliance issues.

Risk ID: R0012 - Unauthorized Access to Investment Portfolios

- Strong Authentication: Implement robust authentication mechanisms, including MFA and strong password policies.
- Access Controls: Restrict access to investment portfolios based on user roles and permissions.
- Activity Monitoring: Continuously monitor user activity for suspicious patterns or unauthorized access attempts.
- Data Encryption: Encrypt sensitive data at rest and in transit to protect against unauthorized access.
- Third-Party Vendor Management: Ensure that third-party service providers have adequate security measures in place to protect customer data.

Risk ID: R0008 - Fraud Detection System Failure

- Regular Testing and Maintenance: Conduct regular testing and maintenance of the fraud detection system to ensure its accuracy and reliability.
- Redundancy: Implement redundant systems to provide backup in case of system failures or outages.
- Continuous Monitoring: Monitor the fraud detection system for performance issues or anomalies.
- Algorithm Updates: Regularly update fraud detection algorithms to stay current with evolving fraud techniques.

- Human Oversight: Maintain human oversight of the fraud detection system to identify false positives or negatives.

# Conclusion

This risk assessment report has identified several critical vulnerabilities that could significantly impact the organization during and after the acquisition of Garden City Wealth Management by Jones & Davis. The risks outlined, including data breaches, credential theft, unauthorized access to sensitive financial information, encryption key theft, non-compliance with data protection regulations, and system failures, highlight the need for immediate attention to cybersecurity measures and regulatory compliance.

Mitigation strategies have been recommended for High Impact risk, emphasizing the importance of robust encryption, multi-factor authentication, regular security audits, and comprehensive employee training to safeguard customer data and maintain the integrity of financial operations. Additionally, the integration of fraud detection systems, proper access controls, and regular compliance reviews will help mitigate the risk of financial fraud, data exposure, and legal repercussions.

By addressing these vulnerabilities through the recommended mitigation strategies, Jones & Davis can reduce the potential for financial losses, reputational damage, and operational disruptions, ensuring a smooth transition and maintaining customer trust. Ongoing vigilance in monitoring and updating cybersecurity practices will be critical in safeguarding the organization against evolving threats.