Cyber Security Management Program

Fabella Bank

Contents

1. Purpose

The purpose of the Cyber Security Management Program at Fabella Bank is to protect the bank's data, technology systems, employees, and customers from cyber threats, fraud and data breaches. This program explains how Fabella Bank will manage cybersecurity risks, respond to incidents and ensure that all digital operations from online banking to internal systems are safe, reliable, and trustworthy.

The program aims to make sure that sensitive customer and company information stays private and accurate while being available whenever needed. It also serves as a guide for employees to follow best security practices, use technology responsibly, and support a culture of awareness and accountability.

Fabella Bank's cybersecurity program also focuses on using modern tools like artificial intelligence for threat detection, biometric authentication for customer logins, and blockchain-based audit trails for high-value transactions. These innovations help the bank stay ahead of emerging cyber risks while providing safer and faster digital banking services.

2. Description of Organization

Fabella Bank is a regional financial institution headquartered in Springfield, Illinois, with three branches across the city. The bank serves both individual and business customers, offering checking and savings accounts, loans, mortgages, investment advice and mobile/online banking services.

Fabella Bank operates both onsite data centers and cloud-based platforms to run its banking systems. The main banking application, called MYBANK, allows customers to perform transactions through the web or mobile app. The older LEGACY BANK system still supports some core operations and syncs data with MYBANK in real time.

The bank employs around 200 staff, including salespeople, IT specialists, risk managers and cybersecurity professionals. The largest branch also manages administrative functions such as HR, payroll and compliance through a cloud-based ERP system known as BANK OFFICE.

What makes Fabella Bank stand out is its commitment to technology innovation and customer safety. The bank recently introduced:

- AI-powered fraud detection, that can spot suspicious transactions instantly.

- Voice and facial recognition login options for secure customer authentication.
- Customer cybersecurity education programs that teach clients how to avoid scams and protect their financial data.
- A “Cyber Savings Vault” system that lets customers store sensitive financial documents securely using encryption and biometric verification.

3. Cyber Security Management Program (CSMP)

The following is the CSMP for Fabella Bank with included elements based on best practices and standards.

Description of overall Program

The Cybersecurity Management Program (CSMP) at Fabella Bank follows best practices from NIST 800-53r5 and CIS Control v8 to create a strong, proactive defense strategy. CSMP helps the bank to identify threats early, respond quickly to incidents, and ensure that both regulatory requirements and customer expectations are met.

The program is overseen by the Chief Information Security Officer (CISO) and supported by an experienced cybersecurity team. Its mission is to protect the Confidentiality, Integrity and Availability of all bank systems and data, while supporting innovation and smooth banking operations.

Security Objectives

- Maintain confidentiality, integrity, and availability of Fabella Bank information based on data classification, business mission, and acceptable level of risk.
- Protect customer data by using strong encryption, secure access controls, and continuous monitoring.
- Maintain uninterrupted banking services through disaster recovery and data backup systems.
- Detect and respond quickly to cyber threats using AI-based monitoring and automated alerts.
- Comply with banking and privacy regulations such as GLBA, PCI DSS and GDPR (for international transactions).
- Educate employees and customers to recognize phishing fraud, and social engineering attacks.

- Adopt advanced security technologies such as blockchain logging and biometric access to stay ahead of emerging cyber threats.

Security Team

Role	Key Responsibilities
Chief Information Security Officer	1) Leads the entire cybersecurity strategy for Fabella Bank. 2) Communicate with top management to align security goals with business objectives. 3) Oversees budgeting, compliance and continuous improvement of the cybersecurity program.
Security Analyst	1) Monitor systems for suspicious activity or potential branches. 2) Reviews security logs and reports to identify trends or vulnerabilities. 3) Works with other departments to fix issues and strengthen defenses.
Network Security Engineer	1) Designs and maintains secure networks for all bank branches and online systems. 2) Configures firewalls, VPNS, and intrusion detection systems (IDS/IPS). 3) Regularly tests the network to identify and fix weak points before attackers exploit them.
Security Administrator	1)Manages user access rights, passwords, and security patches. 2) Installs and maintains antivirus software and security patches. 3)Ensures only authorized staff can access sensitive systems.

Role	Key Responsibilities
Incident Response Analyst	1) Investigates and responds to cybersecurity incidents or alerts. 2) Documents on what happened and how it was resolved. 3) Helps the bank recover quickly and prevent similar incidents.
Risk and Compliance Officer	1)Identifies possible risks to data and systems. 2) Ensures Fabella Bank meets legal and regulatory standards. 3) Updates policies to reduce liability and improve compliance.
IT Support Specialist (Support Role)	1)Provides day-to-day technical support to employees and ensures devices are properly secured. 2) Helps with system updates, password resets, and software troubleshooting. 3) Works with the cybersecurity team to report and resolve technical promptly.

4. Laws, Compliance & Framework Requirements

Laws that apply to Fabella Bank

1. **Gramm-Leach-Bliley Act (GLBA)**
   The GLBA requires banks to protect customers' personal information and explain how it's shared. For Fabella Bank, this law means implementing

privacy notices, encryption for customer data, and security safeguards when sharing information with third-party vendors. It ensures the bank earns customer trust by protecting financial records and personal details.

2. **Sarbanes-Oxley Act (SOX)**
   SOX helps guarantee the accuracy and security of financial reporting. For Fabella Bank, this law means maintaining digital logs, access control, and regular audits of financial systems. Any tampering with records or unauthorized access to accounting data must be prevented through strong cybersecurity measures.

These two laws connect directly to Fabella Bank's goals of transparency, integrity, and customer protection.

Compliance Related Standards

1. **ISO/IEC 27001**
   This global standard provides a framework for creating and managing an **Information Security Management System (ISMS)**. Fabella Bank follows ISO 27001 principles to manage risks, maintain documentation of controls, and improve information security performance. It promotes continual improvement through internal audits and corrective actions.

2. **Payment Card Industry Data Security Standard (PCI DSS)**
   PCI DSS applies to any organization that processes or stores **credit and debit card information**. Since Fabella Bank issues and manages customer cards, compliance with PCI DSS is essential.
   It requires Fabella Bank to:

- Use encryption and firewalls to protect cardholder data.
- Regularly monitor networks for suspicious activities.
- Restrict access to payment data based on job roles.
- Perform annual penetration testing and vulnerability scans.

Following PCI DSS helps prevent card fraud and strengthens customer confidence.

Aligned Standards

These are the standards that this program will be aligned to, or use requirements from:

1. **NIST Special Publication 800-53 Revision 5 (NIST 800-53r5)**
   NIST 800-53r5 outlines a detailed catalog of security and privacy controls used by U.S. federal agencies. Fabella Bank aligns itself to ensure its policies, technologies, and processes meet strong federal-level security expectations. It forms the foundation of the bank's cybersecurity program by defining controls for risk management, access control, incident response, and system monitoring.

2. **FFIEC Cybersecurity Assessment Tool (FFIEC CAT)**
   Developed by the Federal Financial Institutions Examination Council, this tool measures a bank's cybersecurity maturity. Fabella Bank uses it to evaluate how prepared it is against threats, review its risk exposure, and guide yearly improvements in its defenses. It supports compliance with regulators and helps benchmark progress across all branches.

3. **Center for Internet Security (CIS) Controls Version 8**
   CIS Controls v8 provides 18 clear, actionable steps based on real-world attacks. Fabella Bank uses these controls to guide everyday technical practices such as vulnerability management, secure configurations, and malware defense. While NIST provides the big picture, CIS v8 ensures staff follow practical, hands-on actions that keep systems secure day to day.

5. Data Classification Levels

Fabella Bank defines five main data classification levels to ensure all information from employee and client records to payment data is protected based on its sensitivity and importance. These classifications determine who can access the data, how it is stored, and how it is shared within the organization.

Data Classification	Definition	Examples
Public	Information is available to everyone and poses no risk to the bank if shared. It does not contain private or financial details	Bank website, marketing materials, press releases, community newsletters, and public financial statements.
Internal	Information intended for daily internal operations that is not meant for public release but would cause minimal harm if leaked. Accessible to all employees.	Internal announcements, meeting minutes, internal phone directories, general HR policies, and employee schedules
Company Confidential	Non-public information that should only be accessed by specific departments or authorized employees. Unauthorized disclosure could impact operations or business reputation.	Internal finance reports, branch performance data, vendor contracts, risk management documents, and departmental project files.
Private	Personally Identifiable Information (PII) and sensitive data protected under federal or industry regulations. Access is restricted to authorized personnel who handle customer or employee records	Employee personnel files, payroll data, customer account details, client information, payment card data, transaction records, and Social Security numbers.
Restricted	The highest level of protection for data that, if exposed, could cause serious harm to Fabella Bank, its customers, or its partners. Strict encryption, access control, and monitoring are required.	Encryption keys, cybersecurity configurations, system passwords, incident reports, audit logs, legal compliance data, and internal security testing results

6. Security Awareness Program

1. **Annual User Security Awareness Training**

This is the most important activity because it helps employees understand how to recognize and avoid security risks. It should be mandatory for all staff, whether they work in the office or remotely.

***Topics to include in this yearly training*:**

- **Social Engineering**: Is a trick that hackers use to fool people into sharing information.
- **Phishing Awareness**: Once a year, the organization should send out a fake phishing email campaign to test employees' awareness. The goal isn't to punish anyone, it's to identify who might still click on suspicious links and provide extra training.
- **Password Security**: By learning how to create and manage strong passwords.
- **Insider Threats**: To understand that threats can come from within the company.
- **Data Privacy**: How to handle customer and company data safely.
- **Safe Internet and Email Use**: Avoiding risky websites or downloads.
- **Mobile Device Security**: Protecting phones, tablets, and laptops from cyberattacks.
- **Reporting Procedures**: How and when to report suspicious activity or emails.

2. **Annual Cyber Hygiene and Device Security Workshop:**

This hands-on workshop teaches employees how to keep their devices, laptops, phones, and tablets protected from malware or hacking.

***Eight topics to include in this yearly training*:**

- **Software Updates** – Learning that updates fix security holes and reduce risks.
- **Safe USB and External Drive Use** – Avoiding infection from unknown or shared drives.
- **Securing Wi-Fi Networks** – Using secure, encrypted connections and avoiding public Wi-Fi.
- **Strong Device Passwords and Screen Locks** – Preventing unauthorized access to devices.
- **Data Backup Practices** – Saving copies of important data to recover from crashes or attacks.
- **Recognizing Malware Symptoms** – Spotting unusual computer behavior, like slow performance or pop-ups.
- **Using Multi-Factor Authentication (MFA)** – Adding an extra verification step beyond passwords.
- **Protecting Bank-Issued Devices** – Ensuring only approved software is installed on company equipment.

This workshop helps employees apply safe habits to their everyday work.

3. **Annual Policy Review and Update Workshop**

Cyber threats change every year, so company policies shouldn't stay the same. Once a year, the IT and HR departments should hold a policy review meeting where employees can learn about updated rules like acceptable use, data handling, or remote work policies. This keeps everyone informed and ensures compliance with new security standards or regulations.

Eight topics to include in this yearly training:

- **Acceptable Use Policy** – This is by reviewing what's allowed on company devices and networks.

- **Data Classification** – Understanding the difference between public, internal, and confidential data.
- **Cloud Security Rules** – Learning safe practices for using cloud storage.
- **Remote Work Policy** – Setting expectations for security when working off-site.
- **Reporting Data Breaches** – Reviewing steps to follow if a breach occurs.
- **Physical Security** – Remembering to protect access badges, doors, and visitor entry.
- **New Cyber Threat Trends** – Learning about current scams or attack types.
- **Employee Recognition** – Rewarding departments that follow good cybersecurity practices.

These three annual activities training, phishing simulations, and policy reviews work together to keep everyone in the organization aware, prepared, and responsible. By repeating them every year, the bank builds a strong culture where employees don't just rely on technology but actively help protect the organization from cyber threats.

7. Policies

There are many policies that are important to our organization, three of them are within this document.

1. Acceptable Use Policy
2. Asset Management Policy
3. Access Control Policy
4. Risk Management Policy

ACCEPTABLE USE POLICY

Purpose of Policy: The purpose of this policy is to ensure that all Fabella Bank employees, contractors, and partners use the bank's technology and information systems responsibly, securely, and ethically. The goal is to protect both the

organization's data and its reputation from misuse or careless behavior. It also helps employees understand acceptable versus prohibited activities when using bank resources like email, internet, and internal systems.

Scope of Policy: This policy applies to everyone who has access to Fabella Bank's digital resources including full-time employees, interns, consultants, and vendors. It covers the use of all devices, software, and network services owned or managed by the bank. This includes desktop computers, laptops, mobile devices, cloud applications, and remote connections.

Roles and Responsibilities:

- **Employees** must follow all guidelines, avoid prohibited activities, and report security concerns.
- **Managers** are responsible for ensuring their teams are aware of and comply with this policy.
- **IT Security** monitors system usage, detects suspicious behavior, and enforces security measures.
  Together, these roles maintain accountability and promote a consistent security culture across the bank.

Policy Statements:

1. Bank systems and internet access must be used for official business purposes only.
2. Personal use of company equipment should be minimal and not interfere with work.
3. Unauthorized installation or downloading of software is prohibited.
4. Users must never share passwords or login credentials with others.
5. Accessing or distributing inappropriate, illegal, or offensive content is strictly forbidden.
6. Sensitive information cannot be copied, shared, or stored on personal devices.

7. All suspected security issues or data breaches must be reported immediately to IT Security.

8. All user activities on bank systems are subject to monitoring for compliance. These rules help protect the bank's digital environment, ensuring data remains safe and employees act responsibly.

Enforcement/Exceptions: Failure to comply with this policy may result in disciplinary action, which could include access restriction, suspension, or termination of employment. Severe cases may involve legal action if data theft or policy abuse occurs. Exceptions can only be approved in writing by the Chief Information Security Officer (CISO) after careful review of the request.

Last Reviewed / Approved

- Last Reviewed Date: November 2025
- Last Updated Date: November 2025
- Approved By: Fabella Bank, Chief Information Security Officer (CISO)
- Next Review Date: November 2026

ASSET MANAGEMENT POLICY

Purpose of Policy: Fabella Bank establishes this policy to manage risks as they relate to Asset Management. The policy statements describe controls, that when implemented by supporting standards and procedures, are designed to move the associated risks to an acceptable level. This Standard is based on the NIST Special Publications 800-53, Release 5, and Center for Internet Security CIS 8.0.

Scope of Policy: The purpose of this policy is to ensure that all information assets owned or managed by Fabella Bank are identified, tracked, protected, and used properly throughout their life cycle. Managing assets helps prevent data loss, theft, or misuse of critical bank resources. This policy also supports budgeting, compliance, and security operations by maintaining a clear view of all systems and devices in use.

Roles and Responsibilities:

Unless otherwise indicated, all employees, contractors, vendors or other third parties that manage, process or store Fabella Bank data or systems are bound by this policy.

- **IT Asset Manager:** They maintain the central asset inventory and perform regular audits.
- **Department Heads:** Ensure that all assets under their control are properly documented and safeguarded.
- **Employees:** Handle devices carefully, prevent unauthorized use, and report damage or loss immediately.
  Together, these roles ensure that every asset remains accounted for and protected from the moment it's acquired until it's retired or disposed of.

Policy Statements:

[CIS 8:1.1] Inventory and Control of Enterprise Assets | Establish and Maintain Detailed Enterprise Asset Inventory: Fabella Bank will maintain a complete and up-to-date inventory of all devices that store or process bank data, including laptops, mobile phones, servers, and IoT equipment. The IT Asset Manager is responsible for ensuring the accuracy of this inventory to support security and compliance efforts.

[CIS 8:3.6] Data Protection | Encrypt Data on End-User Devices: All sensitive data stored on end-user devices such as laptops and smartphones must be encrypted to prevent unauthorized access or disclosure. Encryption practices ensure that customer and employee information remains secure, even if a device is lost or stolen.

[CIS 8:4.8] Secure Configuration of Enterprise Assets and Software | Uninstall or Disable Unnecessary Services on Enterprise Assets and Software: Fabella Bank will ensure that unnecessary services and software are disabled or removed from all enterprise assets to reduce security risks. Only authorized configurations approved by IT Security may be applied to systems used within the organization.

[CIS 8:4.11] Secure Configuration of Enterprise Assets and Software | Enforce Remote Wipe Capability on Portable End-User Devices: All bank-owned mobile and portable devices must have a remote-wipe capability to protect data in case of theft, loss, or employee separation. This ensures that sensitive information cannot be accessed outside of the bank's control.

[CIS 8:10.1] Malware Defenses | Deploy and Maintain Anti-Malware Software: Anti-malware protection must be installed and actively maintained on all systems and devices connected to the bank's network. Regular scans and threat monitoring help prevent infection and support secure banking operations.

[CIS 8:10.2] Malware Defenses | Configure Automatic Anti-Malware Signature Updates: The IT department must ensure that anti-malware software is automatically updated with the latest signatures. This prevents newly discovered threats from compromising systems and supports overall network health**.**

Enforcement/Exceptions:

Failure to comply with this policy may result in disciplinary action, including loss of access privileges or employment termination. Intentional misuse or theft of assets could lead to legal consequences. Exceptions to this policy must be reviewed and approved by the Chief Information Security Officer (CISO) to ensure they do not introduce unnecessary risk.

Last Reviewed / Approved

- Last Reviewed Date: November 2025
- Last Updated Date: November 2025
- Approved By: Fabella Bank, Chief Information Security Officer (CISO)
- Next Review Date: November 2026

ACCESS CONTROL POLICY

Purpose of Policy:

The purpose of this policy is to define how Fabella Bank manages user access to its systems, networks, and data to protect confidentiality, integrity, and availability. Proper access control ensures that employees can only reach the information necessary for their specific roles, reducing the risk of insider misuse or external attacks. This policy supports compliance with regulatory requirements and industry standards while maintaining customer trust.

Scope of Policy: This policy applies to all employees, contractors, temporary workers, and third parties who access Fabella Bank's systems, applications, or data. It covers

both on-site and remote access to networks, databases, cloud platforms, and other IT resources. The scope extends to any device or connection method that interacts with the bank's environment, including VPNs and mobile applications**.**

Roles and Responsibilities:

- **System Administrators** create, modify, and disable user accounts and access privileges.
- **Department Managers** approve access requests based on job requirements.
- **IT Security Team** monitors access logs, performs regular audits, and enforces compliance.
- **Employees** must protect their login credentials and immediately report any unauthorized access attempts.
  Together, these roles ensure that Fabella Bank maintains strict control over who can access sensitive information.

Policy Statements: Policy Statements (Aligned to NIST 800-53r5 – 8 Clauses)

1. **Authorization of Access**: All user access must be formally requested, reviewed, and approved by a department manager and authorized by the IT Security Team. *(AC-2)*
2. **Least Privilege**: Access rights must be granted only to perform assigned duties and restricted to necessary systems or data. *(AC-6)*
3. **Account Management**: User accounts must be created, modified, or disabled through the approved process maintained by IT Security. *(AC-2)*
4. **Multifactor Authentication (MFA):** MFA is required for all remote, privileged, and administrative accounts. *(AC-17)*
5. **Access Review**: User access permissions must be reviewed semiannually and after role changes or termination. *(AC-2, AC-3)*
6. **Separation of Duties**: No employee should have conflicting access that could allow unauthorized transactions or changes without oversight. *(AC-5)*
7. **Failed Login Attempts**: Systems must lock accounts after a set number of failed login attempts to prevent brute-force attacks. *(AC-7)*

8. **Remote and Mobile Access Control**: Remote access and mobile device connections must use secure VPNs and encryption. *(AC-19)*

Enforcement/Exceptions: Failure to comply with this policy may result in suspension of access privileges, disciplinary action, or termination of employment. Severe violations, such as unauthorized data access or system tampering, may lead to legal action. Any exception to this policy must be documented and approved by the Chief Information Security Officer (CISO) to ensure risk is minimized.

Last Reviewed / Approved

- Last Reviewed Date: November 2025
- Last Updated Date: November 2025
- Approved By: Fabella Bank, Chief Information Security Officer (CISO)
- Next Review Date: November 2026

RISK MANAGEMENT POLICY

Purpose of Policy: The purpose of this policy is to establish a structured approach to identifying, evaluating, and addressing cybersecurity risks that could impact Fabella Bank's operations, systems, and customers. It helps the bank anticipate potential threats and minimize the chances of financial loss, data breaches, or reputational harm. This policy also supports compliance with regulatory frameworks and ensures continuous monitoring of emerging risks**.**

Scope of Policy: This policy applies to all Fabella Bank departments, IT systems, business processes, and third-party vendors. It includes physical, technical, and administrative risks that could affect data confidentiality, integrity, or availability. Every employee, from management to front-line staff, plays a role in recognizing and reporting potential risks that could impact on the bank's cybersecurity posture.

Roles and Responsibilities:

- **Risk Manager:** Oversees the risk management process and maintains the organization's risk register.
- **Department Heads:** Ensure risks identified in their areas are reported, documented, and addressed.

- **Employees:** Must stay alert to suspicious activity and report security incidents or weaknesses immediately.

- **CISO:** Reviews high-risk findings and ensures corrective measures are implemented.
  This collaboration between departments helps the bank maintain a proactive, rather than reactive, approach to managing risk.

Policy Statements (Aligned to NIST 800-53r5 Risk Assessment Family):

1. [RA-3] Risk Assessment: Fabella Bank must conduct an annual risk assessment, including analysis of the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the information asset and the information it processes, stores, or transmits.

- The results of the risk assessment must be documented and reviewed.
- Risk results must be shared with appropriate individuals and teams.
- The Risk Assessment materials must be updated on a documented schedule or at a time where the information system or environment of operation changes in a significant manner to warrant an additional risk assessment.

2. [RA-2] Security Categorization:
All information systems and data at Fabella Bank must be categorized by their sensitivity, value, and impact on operations if compromised. This ensures that appropriate security controls are applied based on the importance of each asset. The classification process should follow the bank's data classification policy and consider regulatory obligations under laws such as GLBA. Each category must be reviewed annually to reflect any organizational or system changes.

3. [RA-5] Vulnerability Monitoring:
Fabella Bank must implement a continuous process to identify, document, and remediate vulnerabilities across its infrastructure, including servers, endpoints, and cloud environments. Regular vulnerability scans must be performed, and results reviewed by IT Security to verify that weaknesses are addressed promptly. Systems with high-risk findings should be patched or mitigated within defined timeframes. This proactive monitoring reduces the likelihood of exploitation by cybercriminals.

4. [RA-7] Risk Response:
All identified risks must have clear mitigation or remediation plans that outline specific actions, responsible parties, and target dates for completion. High and critical risks require management approval for any delay or acceptance. The

bank's Risk Register must be updated to reflect progress on mitigation efforts. Periodic reviews of implemented controls ensure that corrective actions remain effective over time and align with regulatory expectations.

5. [RA-8] Risk Monitoring:
Fabella Bank must maintain ongoing monitoring of risk factors, emerging threats, and control effectiveness. The Risk Manager is responsible for updating the risk register as new risks are identified or existing ones evolve. Quarterly reports will be presented to executive management and the board to ensure accountability. This continuous monitoring enables the bank to adapt its security strategies quickly in response to new challenges and maintain an up-to-date understanding of its risk posture

Enforcement/Exceptions:

Non-compliance with this policy may result in disciplinary action, restricted access to systems, or termination. Significant violations may trigger legal or financial consequences. Any exceptions must be reviewed and approved by the Chief Information Security Officer (CISO) and documented to ensure that they do not introduce unnecessary risks to the organization.

Last Reviewed / Approved

- Last Reviewed Date: November 2025
- Last Updated Date: November 2025
- Approved By: Fabella Bank, Chief Information Security Officer (CISO)
- Next Review Date: November 2026

ADDITIONAL POLICIES

To further strengthen Fabella Bank's cybersecurity governance, the following policies will be created in future updates:

1. Password Policy
2. Data Privacy and Protection Policy
3. Email and Internet Usage Policy
4. Incident Response Policy
5. Business Continuity and Disaster Recovery Policy
6. Physical Security Policy
7. Vendor and Third-Party Security Policy

8.Security Monitoring and Logging Policy

8. Security Controls

These are the information assets that require protection.

Information Assets that Require Protection

Information or Information Asset (name)	How needed by business or mission	System Classification
Email	Used for daily communication between employees, customers, vendors, and leadership. Also used for receiving financial reports, alerts, and internal approvals.	Confidential
Bank Office ERP	Supports HR, payroll, finance, and back-office operations. Holds employee PII, payroll data, and internal financial documents.	Highly Confidential
MYBANK Platform	Main banking applications used by all branches and cloud systems. Supports	Highly Confidential / Mission Critical

Information or Information Asset (name)	How needed by business or mission	System Classification
	customer accounts, transactions, transfers, loan processing, and online/mobile banking	
LEGACY BANK Application	Older backend system is still connected to MYBANK for historical data, reporting, and some batch financial processes.	Confidential
Issued Assets (Laptops and Workstations)	Used by employees to access bank systems, complete transactions, generate reports, communicate, and perform daily work tasks. Holds cache credentials and sensitive operational data.	Internal / Confidential
OneDrive (Microsoft cloud storage)	Used by employees to store work documents, share files securely, collaborate on reports, and access files across devices using Microsoft tools.	Confidential
Loan Setup Applications	Used to process commercial, real estate, auto, and personal loans. Contains customer financial data, credit reports, and approval workflows.	Highly Confidential
Auditing	Supports compliance and internal audits by reviewing transactions, financial statements, and operational data. Ensures regulatory reporting accuracy	Confidential / Regulatory Sensitive
Cash Count	Used to track cash deposits, withdrawals, teller transactions, and daily vault balancing. Supports accuracy and fraud detection.	Confidential / Operational

Security Controls Aligned to Information Assets

This section details the security controls that are implemented or planned to be implemented. We do this by starting with a category of control, and then identifying what should be put into place to protect the information asset.

Reference Enterprise Cybersecurity Architecture Categories

1. System Administration
2. Network Security
3. Application Security
4. Endpoint, Server, and Device Security
5. Identity, Authentication and Access Management
6. Data Protection and Cryptography
7. Monitoring, Vulnerability and Patch Management
8. High Availability, Disaster Recovery, and Physical Protection
9. Incident Response
10. Asset Management and Supply Chain
11. Policy, Audit and Training

In addition to the requirements and data that have been indicated above, these are additional requirements that have been derived to better protect the data described above.

FABELLA BANK YOUR FUTURE, OUR TRUST	**Cyber Security Management Program** **STUDENT NAME: JACINTA IZUNDU**

Information or System that is being protected	**Security Requirement**	**System or Security Control Implemented (category)**	**Control, Tool or Technology**
Email	• Confidentiality, Integrity ➢ Availability	• Identity, Authentication & Access management; Data Protection & Cryptography ➢ Monitoring, Vulnerability & Patch management	• Password Authentication, Encrypted session to email when using Web and Multi-factor authentication ➢ Anti-phishing gateway, spam filters, security patching
Bank Office ERP	• Confidentiality ➢ Integrity ✓ Availability	• Identity, Authentication & Access Management ➢ Data Protection and Cryptography ✓ High Availability & Disaster Recovery	• Role-based access and strong MFA for HR and payroll staff ➢ Encryption at rest in cloud ✓ Cloud redundancy and automated backup

FABELLA BANK YOUR FUTURE, OUR TRUST	**Cyber Security Management Program** **STUDENT NAME: JACINTA IZUNDU**

Information or System that is being protected	Security Requirement	System or Security Control Implemented (category)	Control, Tool or Technology
MYBANK Platform	• Confidentiality, Integrity ➢ Availability	• Application security • Network security ➢ High availability, DR and physical security.	• Secure coding WAF • Network segmentation IDS/IPS ➢ Load balancing, databased replication failover system
LEGACY BANK Application	• Integrity ➢ Confidentiality ✓ Availability	• Monitoring and patch management ➢ System administration ✓ High availability and physical protection	• Vulnerability scanning patching ➢ Restricted admin access ✓ Backup power, secure data center
Issued Assets (Laptops)	• Confidentiality ➢ Integrity ✓ Availability	• Endpoint and device security ➢ Monitoring and patch management ✓ Identity and Access management	• Full disk encryption ➢ Auto patching, Vulnerability scanning ✓ MFA, Strong password

FABELLA BANK YOUR FUTURE, OUR TRUST	**Cyber Security Management Program** **STUDENT NAME: JACINTA IZUNDU**

Information or System that is being protected	Security Requirement	System or Security Control Implemented (category)	Control, Tool or Technology
OneDrive	• Confidentiality ➢ Integrity ✓ Availability	• Data protection ➢ Identity and access management ✓ High availability	• Cloud encryption and restricted access ➢ MFA, conditional access ✓ Cloud redundancy and version history
Loan Setup Applications	• Confidentiality ➢ Integrity ✓ Availability	• Application security ➢ Data protection ✓ High availability	• RBAC, Secure coding ➢ Encryption and audit trails ✓ Backups and redundancy
Auditing	• Integrity ➢ Confidentiality ✓ Availability	• Policy, Audit and Training ➢ Identity and access management ✓ High availability	• Logging, Review processes ➢ RBAC, MFA ✓ Backups, Retention
Cash Count	• Integrity ➢ Confidentiality ✓ Availability	• Monitoring and patch management ➢ Network security ✓ High availability, physical protection	• Logging, alerts ➢ Segmentation, firewalls ✓ Redundant system, secure vault controls

9. Security Operations

Security Operations Run Book

Periodic Check	Frequency	Reason for check	Expected Result
SIEM Alert Review	Daily	Detect early indicators of attacks or unauthorized access.	All high/critical alerts are reviewed and addressed immediately.
Endpoint Protection Status Check	Daily	Ensures antivirus and anti-malware protection is active	All devices show healthy protection and updated signatures.
Network Traffic Monitoring	Daily	Identify unusual traffic that may indicate intrusion.	No abnormal spikes or suspicious outbound connections
Backup Completion & Integrity Verification	Weekly	Ensure data can be restored during ransomware or outages.	Backups run successfully with no corruption
Sensitive System Access Log Review	Weekly	Detect unauthorized or unusual	All access aligns with authorized roles only.
Patch Status Review	Weekly	Prevent exploitation by unpatched vulnerabilities	All critical patches deployed within policy timeframe.
User Account Review & De Provisioning	Monthly	Remove inactive or terminated employee accounts	All inactive accounts disabled or deleted.
Firewall Rule Review	Monthly	Avoid overly broad access and maintain segmentation.	Only approved and necessary rules remain active.
Email Security & Phishing Trend Review	Monthly	Prevent phishing attacks and compromised inboxes.	No compromised accounts: trends show improvement.
Third Party Vendor Security Review	Quarterly	Vendors can introduce supply chain risks	All vendors remain compliant and pose no new risks.

Vulnerability Management

Vulnerability management is like routinely checking all the bank's computers, systems, and apps to make sure there are no "cracks" that hackers could use to break in. Fabella Bank follows the NIST **RA-5 Vulnerability Scanning** control, which simply means we must regularly scan, find, fix, and re-check any weaknesses before cybercriminals can take advantage of them.

[RA-5] Vulnerability Scanning: Fabella Bank has established a clear vulnerability management process that aligns with NIST RA-5 guidelines, and these are the steps below:

5 Process Steps

1. **Identify and Inventory Assets** – Fabella bank keeps a full list of every device, system, application, and cloud service it owns. This prevents unknown or unmanaged devices that attackers often target. Inventory Assets; Fabella Bank maintains a complete inventory of all servers, endpoints, databases, applications, and cloud services. This ensures that every asset is included in scanning and prevents blind spots that attackers can exploit.

2. **Perform Regular Vulnerability Scans** – Automated tools scan computers, servers, networks, and apps for weaknesses. Scans run on a schedule and anytime new threats appear. Regular Vulnerability Scans; automated internal and external scans are performed on a scheduled basis and whenever new threats or vulnerabilities are discovered. Scans include systems, cloud services, applications, configurations, and networks.

3. **Analyze and Prioritize Findings** – The scan results are reviewed and sorted based on how serious each issue is. Problems affecting customer data or core banking systems are fixed first. Prioritize Findings; Vulnerability results are reviewed and prioritized using CVSS scores,

exploitability, business impact, and asset classification. Critical issues on MYBANK, ERP, and customer-facing systems are addressed first.

4. **Remediate and Patch Vulnerabilities** – IT teams fix issues by installing patches, updating configurations, or adding extra protections. The goal is to reduce how long systems remain exposed. Patch Vulnerabilities; IT teams apply patches, configuration changes, or compensating controls. Fabella Bank follows defined SLAs to ensure critical vulnerabilities are fixed quickly to reduce attack exposure.

5. **Validate, Re-Scan, and Report** – After remediation, the systems are scanned again to confirm issues are resolved. Reports are shared with management to track progress and remaining risks. Validate, Re-Scan, and Report; Once remediation is complete, the affected systems are rescanned to confirm vulnerabilities are resolved. Reports are shared with management to track closure rates, recurring issues, and overall risk trends.

Additional best practices such as annual penetration testing, secure configuration baselines, and threat intelligence integration further strengthen the bank's vulnerability management program. such as annual penetration testing, secure configuration baselines, and threat intelligence integration further strengthen the program. such as penetration testing, secure configuration baselines, and threat intelligence integration can further strengthen the program.

10. Continuity Planning

Cyber Incident Response Planning

This section will document key items regarding incident management preparation and response. Before an incident happens, Fabella Bank must be fully prepared. The following five preparation steps ensure the bank can respond quickly and reduce damage.

Preparation

1. Define and Train the Incident Response Team (IRT)

Fabella Bank assigns a trained team responsible for handling cyber incidents. Each member understands their role, duties, and escalation steps.

Outcome: When an incident occurs, the right people respond immediately with no confusion.

2. Establish Clear Communication Channels

Dedicated phone numbers, secured messaging groups, and emergency email procedures are created for staff, leadership, and third parties.

Outcome: Communication flows smoothly, and no time is lost trying to reach the right people.

3. Create and Maintain System Inventories

A complete list of systems, servers, applications, and cloud services is maintained, including who owns each system.

Outcome: During an incident, teams quickly know which systems are affected and who to contact.

4. Develop and Test Backup & Recovery Procedures

Regular backups are performed and tested to make sure data can be restored after ransomware or system failure.

Outcome: Data can be recovered quickly, reducing downtime and financial loss.

5. Develop and Test Backup & Recovery Procedures

Regular backups are performed and tested to make sure data can be restored after ransomware or system failure.

Outcome: Data can be recovered quickly, reducing downtime and financial loss.

High Level Incident Response Plan

Incident Lifecycle	Key Activities
Detection	1. Monitor alerts from SIEM, email security, and endpoint tools. Outcome: Early warning signs of an attack are identified before major damage occurs. 2. Employees report suspicious activity immediately (phishing emails, strange pop-ups). Outcome: Human detection adds an extra layer of protection. 3. Confirm whether the alert is real or a false positive. Outcome: Only true incidents are escalated, improving accuracy and response time.
Analysis	1. Determine what systems, accounts, or data are affected. Outcome: The bank understands the size and seriousness of the incident. 2. Preserve relevant logs and evidence. Outcome: Critical forensic data is protected for investigation. 3. Assess the potential business impact. Outcome: The bank prioritizes the incident correctly based on risk.

Incident Lifecycle	Key Activities
Containment	1. Assess the potential business impact. Outcome: The bank prioritizes the incident correctly based on risk. 2. Block malicious IP addresses, URLs, or email senders. Outcome: Stops ongoing harmful activity 3. Activate emergency communication plan to notify leadership. Outcome: Executives receive immediate visibility into the situation.
Eradication	1. Remove malware, delete malicious files, or disable compromised accounts. Outcome: The threat is fully removed from the environment. 2. Apply missing patches or configuration fixes. Outcome: Strengthens systems so the same attack cannot happen again. 3. Scan all affected systems again to verify removal. Outcome: Confirmation that the environment is clean.
Recovery	1. Restore clean backups or rebuild affected systems. Outcome: Services return to normal with no leftover infection. 2. Monitor systems closely for re-infection or unusual behavior. Outcome: Ensures the threat does not return. 3. Notify customers or regulators if required (GLBA or state law). Outcome: Compliance obligations are met and trust is maintained.

Incident Lifecycle	Key Activities
Post Incident Activity	1. Hold a post-incident meeting within 7–10 days. Outcome: The team discusses what worked and what can be improved. 2. Update policies, controls, or configurations based on the incident. Outcome: The bank becomes stronger and reduces the chance of repeat issues. 3. Document the full incident report. Outcome: Provides evidence for audits, regulators, and internal learning.

Business Continuity Planning

The purpose of Fabella Bank's Business Continuity Planning is to ensure the bank can continue providing essential services even when major disruptions occur. BCP focuses on protecting customers, keeping employees safe, and restoring operations as quickly as possible. By planning for different scenarios, the bank reduces confusion and financial loss during emergencies. Business Continuity Planning ensures that Fabella Bank continues operating even during emergencies.

Scenario	High Level First Effort Response
Internet Goes Down Across the Bank	Why this is a problem: Cloud systems and online banking become unavailable. Response: Switch to backup ISP, use manual forms, confirm outage details. Communication: SMS to staff and notice to customers.
Ransomware Attack Freezing Critical Systems	Why this is a problem: MYBANK and LEGACY may become unusable. Response: Isolate devices, activate IR team, restore backups. Communication: Notify staff, leadership, and customers if needed.
Flooding Damages the Data Center	Why this is a problem: Hardware and servers may be destroyed. Response: Switch to off-site backup center, restore applications, ensure safety. Communication: Emergency alerts to staff, notify regulators.

Cloud Outage Affecting Online/Mobile Banking	Why this is a problem: Customers cannot access digital services. Response: Activate backup cloud region, provide limited offline mode. Communication: Update website and customer support scripts.
Power Failure at Main Branch or HQ	Why this is a problem: Branch operations and ATMs may shut down. Response: Activate generators and UPS, move critical staff temporarily. Communication: Alert staff and inform customers only if services are disrupted.

11. Risk Management

Risk Definition

This is the risk definition for our enterprise.

Impact Scores	Mission	Operational Objectives	Obligations
Definition	*My Bank exists to provide secure, reliable, and accessible financial services to customers in the Springfield area. Its mission is to protect customer funds, support financial growth, and maintain trust through safe and modern banking technology*	*• Keep banking systems like MYBANK, ERP, ATMs, and mobile apps running smoothly.* *• Protect customer and employee information from unauthorized access.* *• Ensure daily operations such as deposits, withdrawals, loan processing, payroll, and reporting run without disruption.* *• Maintain compliance with financial and cybersecurity regulations.*	*• Protect customer data (PII, account details, transactions).* *• Ensure fair and uninterrupted access to financial services.* *• Report breaches or outages to regulators when required.* *• Prevent harm to customers, employees, and third-party partners*
1 - Negligible	A small disruption occurs but does not affect customers or the bank's ability to serve them.	Routine work may slow down briefly but returns to normal without extra effort.	No harm to customers or partners; no regulatory action required.
2. Acceptable	The bank can still achieve its mission with little or no impact on customer trust	Minor issues may require small adjustments but no major cost or downtime	No harm to customers, and any inconvenience is easily corrected.

Impact Scores	Mission	Operational Objectives	Obligations
3. Unacceptable	The bank must reinvest time or money to fix the situation before it can continue serving customers reliably	Operations are disrupted enough that extra resources or overtime work are needed to catch up.	Customers or partners may experience temporary harm or delayed services, but the harm is fixable.
4 - High	The bank's ability to provide services is significantly affected for an extended time	Key systems become unavailable, causing major downtime, financial loss, or regulatory concerns.	Customers may face real impacts such as delayed transactions, financial stress, or other risks.
3. Catastrophic	The bank cannot achieve its mission, and customer trust is severely damaged.	Critical systems fail completely, operations stop, and recovery requires full restoration efforts	Harm to customers or partners is long-lasting or not fully correctable; regulators may intervene.

Risk Assessment

Latest Risk Assessment Report and Remediation Plan

Measurement	Value
Date of Risk Assessment	Q2 2023
Number of controls reviewed	40
Number of risks acceptable (green)	30
Number of risks unacceptable (yellow)	4
Number of risks critical (red)	6

High Level Remediation Plans

The following safeguards listed below here provide targeted risk-reduction strategies for each control that exceeded the acceptable risk rating:

Remediation Plans
Enforce Automatic Device Lockout on Portable End-User Devices
Enforce Remote Wipe Capability on Portable End-User Devices
Establish an Access Revoking Process
Perform Automated Vulnerability Scans of Internal Enterprise Assets

Remediation Plans
Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets
Configure Automatic Anti-Malware Signature Updates
Perform Automated Backups
Train Workforce on Data Handling Best Practices
Perform Root Cause Analysis on Security Vulnerabilities
Conduct Routine Incident Response Exercises

END OF DOCUMENT