Risk Assessment

Component	Threat	Current State
Establish and Maintain a Data Management Process	Data is leaked, lost, or accessed by inappropriate personnel or attackers / malicious actors.	File shares are open to all employees, there is no formal process for the organiation of data, no written policy exists, no single administrator is responsible for data management.
Establish and Maintain a Data Inventory	Lack of awareness around what data is stored can cause inability to fix vulnerability	Data inventory is currently ad-hoc, with some information kept at a high level in SharePoint, but no additional formal data inventory maintained at the organziational level of ATM and Internet Banking (IB) databases.
Securely Dispose of Data	Data is leaked if not disposed of securely	The "Data Desctruction and Classification" policy states that all physical drives (CD, USB, Flash, and Hard Disk) must be wiped using secured methods and then physically destroyed. There is no planned rotation of physical disks within IB and ATM systems upcoming.
Encrypt Sensitive Data in Transit	Unencrypted data can be intercepted and sensitive data revealed	Network traffic over TCP to ATMs is is through HTTPS APIs and encrypted. Data between the IB server and core banking systems is through internal network and not encrypted. Older ATMs using modem communication is not encrypted.
Log Sensitive Data Access	Unauthorized access to sensitive data or insider threats to system integrity	All access to the core banking system is logged with database, administrative access, and transactions all kept in separate logging facilities on the system itself. Acess to Internet Banking server over RDP for management access is logged.
Establish and Maintain an Inventory of Accounts	Proper access controls must be in place to prevent improper access to sensitive data	An inventory of all users with access directly to the core system is maintained within the system itself, an access review is conducted annually for all of these users and accounts, with the direct manager being required to sign off on their access for the upcoming year.
Use Unique Passwords	Passwords that can be easily guessed can allow threat actors to access employee or customer accounts	Core banking system requires the use of strong passwords (10 characters, full complexity, rotated every 30 days). Internet Banking and ATM servers require the same for administrators. Customer accounts for Internet Banking do require complexity but passwords are only forced to reset in the event of an issue.
Disable Dormant Accounts	Dormant accounts that still have access to sensitive data can be used as vectors for intrusion by threat actors	A process is being implemented to identify dormant employee acounts which may no longer be needed, but it is not implemented at this time.
Establish an Access Granting Process	Unauthorized access to data or customer accounts	As noted in the "Access Management" policy, dated and approved by the board in Jan 2012, all access to Core Banking systems (including IB and ATM), but be submitted via ticket request. A formal approval process is then the first step of this process, to validate only access available where needed.

Risk Assessment

Component	Threat	Current State
Require MFA for Externally-Exposed Applications	Unauthorized access to customer accounts	Multifactor is not required for customer access to Internet Banking services; however, per FFIEC requirements a process is being developed to implement this in 2023 after customer impact is taken into account. Technical solutions have been evaluated and customer acceptance testing groups are being formed.
Require MFA for Remote Network Access	Unauthorized access to sensitive data	Remote access to manage core banking systems is not allowed through our VPN. Employees must either report to an office or branch locaton to perform any engineering or administrative capabilities.
Standardize Time Sychronization	Inability to communicate between devices due to time differences	All Windows servers (ATM, Internet Banking, and IB database) are configured as part of Active Directory. Core Banking systems are configured to utilize NTP against the Active Directory Domain Controllers for time sync.
Deploy and Maintain Anti-Malware Software	Malware	Network monitoring software, including IDS/IPS, has been deployed in front of the Internet facing web server as part of the Internet Banking service. Anti-Virus nor EDR has been configured on any of our servers, including ATM, IB, and Core.
Disable Autorun and Autoplay for Removable Media	Malware installed on removable media	Removable media is not allowed to be utilized against the core servers per the "Removable Media" policy. The AS400 operating system upon which the core operates does not allow for technical controls; however, the system is physically secured reducing the overall risk.
Designate Personnel to Manage Incident Handling	Incident response lacking direction could lead to ineffective response	As per the business continuity plan and Incident Response Plan, all IR decisions must be made through the Continuity Committee, which consists of several managers, executives, and representatives from core business functions, including branch operations, IT, core systems, and application development.
Assign Key Roles and Responsibilities	Unorganized team may be ineffective in facing threats	A Chief Information Security Officer has been defined within the Information Security Program as required by GLBA and FFIEC requirements.
Establish and Maintain a Secure Application Development Process	Vulnerabilities in an application can lead to exploitation in the future	All changes to Core and Internet Banking (IB) systems must first be approved through a change management request ticket. Changes must be pushed into revision control where they are then implemented in a test enviroment for at miniumum of 30 days. Emergency changes can be approved by the CIO and CBO (Chief Banking Officer).
Use Standard Hardening Configuration Templates for Server Infrastructure	Bad configuration leads to vulnerabilities in application servers	New application servers (including ATM and IB) are built from a standard baseline image. All new builds must then be hardened using the "Standard Server Hardening Guide" as developed and maintained by IT.

Risk Assessment

Component	Threat	Current State
Separate Production and Non-Production Systems	Changes made to production systems are publicly-facing and can be exploited if insecure	A separate test environment is maintained for Internet Banking system development. The ATM server does not currently have a test environment for change management; however, changes are minimal and limited to updates from the vendor.
Train Developers in Application Security Concepts and Secure Coding	Vulnerabilities in code may lead to applications being exploited	All developers are provided Information Security training as part of the organizations annual training and compliance package that all employees are required to attend. Additional updates are given by the Information Security team during some of the dev team meetings.
Conduct Penetration Testing	Having unknown vulnerabilities in production systems can be exploited	Internal and External Penetration Assessments are performed against the bank network on an annual basis as part of the ongoing audit plan.

Risk Assessment

Component	Data Type	Data Volume	Impact	Likelihood
Establish and Maintain a Data Management Process	Confidential	Minimal (<5,000)	High (>$200k, enterprise / infrastructure, loss of life)	High (Highly Likely or 10-100 times per year)
Establish and Maintain a Data Inventory	Internal	Moderate (20,000 - 100,000)	Moderate ($50k - $200k, organizational / service level)	Moderate (Somewhat Likely or 1-10 times per year)
Securely Dispose of Data	Confidential	Minimal (<5,000)	Moderate ($50k - $200k, organizational / service level)	Low (Unlikely or less than once a year)
Encrypt Sensitive Data in Transit	Restricted	High (>100,000)	High (>$200k, enterprise / infrastructure, loss of life)	Moderate (Somewhat Likely or 1-10 times per year)
Log Sensitive Data Access	Confidential	Low (5,000 - 20,000)	Low (<$50k, system / team level)	Low (Unlikely or less than once a year)
Establish and Maintain an Inventory of Accounts	Confidential	Moderate (20,000 - 100,000)	Moderate ($50k - $200k, organizational / service level)	Low (Unlikely or less than once a year)
Use Unique Passwords	Confidential	Minimal (<5,000)	Moderate ($50k - $200k, organizational / service level)	High (Highly Likely or 10-100 times per year)
Disable Dormant Accounts	Internal	Minimal (<5,000)	Moderate ($50k - $200k, organizational / service level)	Low (Unlikely or less than once a year)
Establish an Access Granting Process	Confidential	Moderate (20,000 - 100,000)	High (>$200k, enterprise / infrastructure, loss of life)	Low (Unlikely or less than once a year)

Risk Assessment

Component	Data Type	Data Volume	Impact	Likelihood
Require MFA for Externally-Exposed Applications	Confidential	High (>100,000)	Moderate ($50k - $200k, organizational / service level)	Moderate (Somewhat Likely or 1-10 times per year)
Require MFA for Remote Network Access	Restricted	Moderate (20,000 - 100,000)	Moderate ($50k - $200k, organizational / service level)	Minimal (Highly Unlikely; once every 10 years)
Standardize Time Sychronization	Public	Minimal (<5,000)	Low (<$50k, system / team level)	Minimal (Highly Unlikely; once every 10 years)
Deploy and Maintain Anti-Malware Software	Confidential	High (>100,000)	High (>$200k, enterprise / infrastructure, loss of life)	High (Highly Likely or 10-100 times per year)
Disable Autorun and Autoplay for Removable Media	Internal	Low (5,000 - 20,000)	High (>$200k, enterprise / infrastructure, loss of life)	Low (Unlikely or less than once a year)
Designate Personnel to Manage Incident Handling	Internal	Minimal (<5,000)	Moderate ($50k - $200k, organizational / service level)	Low (Unlikely or less than once a year)
Assign Key Roles and Responsibilities	Public	Minimal (<5,000)	Moderate ($50k - $200k, organizational / service level)	Minimal (Highly Unlikely; once every 10 years)
Establish and Maintain a Secure Application Development Process	Confidential	Minimal (<5,000)	Moderate ($50k - $200k, organizational / service level)	Moderate (Somewhat Likely or 1-10 times per year)
Use Standard Hardening Configuration Templates for Server Infrastructure	Confidential	Minimal (<5,000)	Moderate ($50k - $200k, organizational / service level)	Low (Unlikely or less than once a year)

Risk Assessment

Component	Data Type	Data Volume	Impact	Likelihood
Separate Production and Non-Production Systems	Confidential	Minimal (<5,000)	Low (<$50k, system / team level)	Low (Unlikely or less than once a year)
Train Developers in Application Security Concepts and Secure Coding	Internal	Minimal (<5,000)	Moderate ($50k - $200k, organizational / service level)	Low (Unlikely or less than once a year)
Conduct Penetration Testing	Confidential	Moderate (20,000 - 100,000)	Moderate ($50k - $200k, organizational / service level)	Moderate (Somewhat Likely or 1-10 times per year)

Risk Assessment

Component	Control Effectiveness	Overall Risk	Notes
Establish and Maintain a Data Management Process	Low (Detective only, no alerting)	High	Although volume of potential data loss to external sources is minimal, potential impact and likelihood are high. In this case, the minimal controls implemented, lack of written policies, and lack of focused personnel drives this to a high residual risk.
Establish and Maintain a Data Inventory	Low (Detective only, no alerting)	Moderate	Lack of organized data inventory may lead to loss of sensitive data
Securely Dispose of Data	High (Advanced preventative controls and alerting)	Low	The policy states that all physical drives must be wiped then destroyed, which encompasses different data types. There is minimal data volume because there is no planned rotation of disks. This results in a low overall risk
Encrypt Sensitive Data in Transit	Moderate (Some advanced controls or alerting)	High	High data volumes and the existence of unencrypted channels of communication makes this a high risk to the organization, despite some controls in place
Log Sensitive Data Access	High (Advanced preventative controls and alerting)	Low	Controls are highly effective and likelihood of a person with access to sensitive data acting as an insider threat is low enough to give a low overall risk
Establish and Maintain an Inventory of Accounts	High (Advanced preventative controls and alerting)	Low	Insider threats are fairly unlikely and the access is reviewed each year to purge incorrectly set access controls
Use Unique Passwords	High (Advanced preventative controls and alerting)	Low	The password policy is effective in its reset requirement, so overall risk is low. Monthly reset also decreases effective time of stolen credential attacks.
Disable Dormant Accounts	None (No controls in place)	Moderate	The likelihood of a dormant account being used in an attack is low, but there are no controls in place to prevent this from happening
Establish an Access Granting Process	High (Advanced preventative controls and alerting)	Low	There are effective access controls in place for use of the central banking system so the overall risk is low despite a high potential impact

Risk Assessment

Component	Control Effectiveness	Overall Risk	Notes
Require MFA for Externally-Exposed Applications	None (No controls in place)	High	The risk is not controlled at present, but the impact is limited to customer accounts. Look for an improvement in controls in the future.
Require MFA for Remote Network Access	High (Advanced preventative controls and alerting)	Minimal	The policy prevents anyone from logging in without being physically present
Standardize Time Sychronization	High (Advanced preventative controls and alerting)	Minimal	There does not need to be any attempt to hide time, and all systems are synced to a single authority for the network
Deploy and Maintain Anti-Malware Software	Low (Detective only, no alerting)	Critical	Antimalware should be installed on all systems regardless of their exposure to the Internet. Lack of antivirus software on internal systems could allow malware to spread throughout network once inside.
Disable Autorun and Autoplay for Removable Media	Moderate (Some advanced controls or alerting)	Low	Physical controls on the core servers and diminishing use of removable media makes this a low risk for the organization
Designate Personnel to Manage Incident Handling	High (Advanced preventative controls and alerting)	Low	The policy assigns several people to oversee incident response, but effectiveness is dependent on their knowledge of their roles and responsibilities during a security incident
Assign Key Roles and Responsibilities	High (Advanced preventative controls and alerting)	Minimal	The company has a CISO in accordance with the relevant legal requirements
Establish and Maintain a Secure Application Development Process	High (Advanced preventative controls and alerting)	Low	Isolation of test changes before release protects from much of what causes the risk of application-based attacks
Use Standard Hardening Configuration Templates for Server Infrastructure	Moderate (Some advanced controls or alerting)	Moderate	Risk depends on the effectiveness and maintenance of the template used. A bad template could affect the entire network of application servers, moderate risk due to this possibility.

Risk Assessment

Component	Control Effectiveness	Overall Risk	Notes
Separate Production and Non-Production Systems	Moderate (Some advanced controls or alerting)	Low	Risk is due to reliance on ATM vendor for updates when necessary, otherwise low risk on internally controlled systems
Train Developers in Application Security Concepts and Secure Coding	Moderate (Some advanced controls or alerting)	Low	Low risk despite controls that could be better. Other controls effective in this case but should do more to train for secure programming than hold occasional meetings
Conduct Penetration Testing	High (Advanced preventative controls and alerting)	Low	Multiple annual penetration tests serve as a good defense against improper security controls.