**Information Assurance Plan**

For Across the States Bank

Austin Schwalbe

07/14/2024

# Document Properties

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Author** | **Date** | **Description** |
| v1.0 | Austin Schwalbe | 07/14/2024 | Final version |

# Executive Summary

This document outlines the steps Across the States Bank must take to provide information assurance throughout the company network. This will provide company systems and data with support for the CIA triad, ensuring they are kept safe and accessible. It also outlines the teams and steps involved in risk management and incident response, ensuring that business operations can continue in the event of a cyberattack. The purpose of this document is to keep data protected from unauthorized access and changes, minimize the overall attack surface, and ensure an efficient incident response and recovery process.

# Key Terms

* “the company” – Across the States Bank
* “systems” – Computers, access points, servers, and other computing hardware that are owned and operated on the Across the States Bank’s network
* “assets” – Systems, data, and services that are owned, operated, and/or hosted by Across the States Bank
* “critical assets” – Assets that Across the States Bank relies on for day-to-day operations and business with customers

**Table of Contents**

[Document Properties 2](#_Toc171795077)

[Executive Summary 2](#_Toc171795078)

[Key Terms 2](#_Toc171795079)

[1.0 Introduction 5](#_Toc171795080)

[1.1 Overview 5](#_Toc171795081)

[1.2 Scope 5](#_Toc171795082)

[1.3 Purpose 5](#_Toc171795083)

[2.0 Objectives 6](#_Toc171795084)

[2.1 Goals 6](#_Toc171795085)

[2.2 Updates 6](#_Toc171795086)

[2.3 Non-compliance 6](#_Toc171795087)

[3.0 Roles & Responsibilities 7](#_Toc171795088)

[3.1 Security Operations Center 7](#_Toc171795089)

[3.2 Digital Forensics Team 7](#_Toc171795090)

[3.3 Computer Security Incident Response Team 7](#_Toc171795091)

[3.4 Executives 7](#_Toc171795092)

[4.0 Critical Assets, Applications, and Resources 8](#_Toc171795093)

[4.1 Identification 8](#_Toc171795094)

[4.2 Inventory 8](#_Toc171795095)

[4.2.1 Systems 8](#_Toc171795096)

[4.2.2 Data 8](#_Toc171795097)

[4.2.3 Applications 8](#_Toc171795098)

[5.0 Risk Assessment 9](#_Toc171795099)

[5.1 Risk analysis meetings 9](#_Toc171795100)

[5.1.1 Identify potential risks 9](#_Toc171795101)

[5.1.2 Estimate impact of risks 9](#_Toc171795102)

[5.1.3 Report risks 9](#_Toc171795103)

[5.1.4 Devise a solution 9](#_Toc171795104)

[5.2 Vulnerability scanning 9](#_Toc171795105)

[5.3 Penetration testing 9](#_Toc171795106)

[6.0 Ongoing Vulnerability Assessment 11](#_Toc171795107)

[6.1 Vulnerability scans 11](#_Toc171795108)

[6.2 Site surveys 11](#_Toc171795109)

[6.3 Phishing simulations 12](#_Toc171795110)

[6.4 Code analysis 12](#_Toc171795111)

[7.0 Risk Reduction 14](#_Toc171795112)

[7.1 Gap analysis 14](#_Toc171795113)

[7.2 Patch management 14](#_Toc171795114)

[7.3 System upgrades 14](#_Toc171795115)

[7.4 Platform diversity 14](#_Toc171795116)

[8.0 Incident Response Planning 15](#_Toc171795117)

[8.1 Preparation 15](#_Toc171795118)

[8.1.1 Backup systems 15](#_Toc171795119)

[8.1.2 Configuring SIEM tools and log aggregation 15](#_Toc171795120)

[8.1.3 Implement technical controls 15](#_Toc171795121)

[8.1.4 Segment networks 16](#_Toc171795122)

[8.1.5 Train employees 16](#_Toc171795123)

[8.2 Detection & analysis 16](#_Toc171795124)

[8.2.1 Continuous analysis 16](#_Toc171795125)

[8.2.2 Escalation 16](#_Toc171795126)

[8.3 Containment 16](#_Toc171795127)

[8.3.1 Short-term 16](#_Toc171795128)

[8.3.2 Forensics 17](#_Toc171795129)

[8.3.3. Long-term 17](#_Toc171795130)

[8.4 Eradication 17](#_Toc171795131)

[8.4.1 Disable systems 17](#_Toc171795132)

[8.4.2 Scan systems 17](#_Toc171795133)

[8.4.3 Mitigate vulnerabilities 17](#_Toc171795134)

[8.5 Recovery 18](#_Toc171795135)

[8.5.1 Apply backups 18](#_Toc171795136)

[8.5.2 Check configurations 18](#_Toc171795137)

[8.5.3 Continue monitoring 18](#_Toc171795138)

[8.6 Post-incident activity 18](#_Toc171795139)

[8.6.1 Reporting 18](#_Toc171795140)

[8.6.2 Meeting 18](#_Toc171795141)

[8.6.3 Changes 19](#_Toc171795142)

[9.0 Business Continuity & Recovery 20](#_Toc171795143)

[9.1 Business Continuity 20](#_Toc171795144)

[9.1.1 Reroute traffic 20](#_Toc171795145)

[9.1.2 Implement physical alternatives 20](#_Toc171795146)

[9.1.3 Configure alternate communication channels 20](#_Toc171795147)

[9.2 Business Recovery 21](#_Toc171795148)

[9.3.1 Prioritize critical systems 21](#_Toc171795149)

[9.3.2 Restore from backups 21](#_Toc171795150)

[9.3.3 Reset credentials 21](#_Toc171795151)

[9.4.4 Review response 21](#_Toc171795152)

[10. Conclusion 22](#_Toc171795153)

[11. References 23](#_Toc171795154)

# 1.0 Introduction

## 1.1 Overview

The following sections outline the various steps that should be taken by the company to provide a well-rounded information assurance plan. This includes the teams involved, the risk and vulnerability management process, and the incident response process.

## 1.2 Scope

This document covers all systems within the company’s network as well as the data stored on them. It also involves the employees who will be responsible for managing the systems and related processes.

## 1.3 Purpose

The purpose of this document is to support the CIA triad for all of the company’s data and systems. It also aims to mitigate risk by reducing the attack surface as well as provide an efficient response process that supports the continuity and recovery of business operations.

# 2.0 Objectives

## 2.1 Goals

This information assurance plan aims to achieve the following objectives:

* Protect the privacy and security of customers and employees
* Uphold the CIA triad for all data stored on the company network
* Increase efficiency during the incident response process
* Minimize downtime during a cyber incident
* Ensure employees are equipped to handle a cyber event
* Provide greater visibility into the network for greater detection of IoCs
* Ensure business operations are restored as efficiently as possible after a cyber incident

## 2.2 Updates

The Chief Information Security Officer will be responsible for reviewing and updating this policy bi-annually (every six months) to maintain compliance with current industry standards and legal requirements. Certain aspects of this policy (such as the incident response process) may be updated out-of-band as needed.

## 2.3 Non-compliance

Employees who do not comply with the terms of this policy may be subject to loss of privileges, disciplinary/legal action, and/or up to (or including) termination of employment and referral for criminal prosecution.

# 3.0 Roles & Responsibilities

## 3.1 Security Operations Center

**Sr. SOC Operator: Alyssa Green**

Detects potential indicators of cyberattacks and reports them to the Computer Security Incident Response Team (CSIRT) for analysis.

**SOC Analysts: Mark Laurence, Paris Hill, Jennifer Prince**

Responsible for analyzing aggregated logs and packet captures for IoCs – Reports findings to the Sr. SOC Operator.

## 3.2 Digital Forensics Team

**Sr. Forensic Analyst: Benjamin Wells**

Responsible for leading forensics investigations on affected systems after they have been contained during a cyberattack.

**Digital Forensics Analysts: Christine Cox, Daniel Lear, Forrest Gears**

Responsible for executing forensics investigations on affected systems – Determine TTPs, goals, and motivations

## 3.3 Computer Security Incident Response Team

**Head of CSIRT: Jonathan Bourne**

Responsible for initiating and leading incident response process in the event of a cyberattack

**CSIRT First Responders: Alexander Lynx, Kelly Lex**

Responsible for responding to attack indicators sent from SOC Analysts – Determine whether a cyberattack has occurred and report findings to Head of CSIRT.

## 3.4 Executives

**Chief Information Security Officer: Lauren Gray**

Responsible for overseeing the incident response process and post-incident activities – Also responsible for updating the information assurance policy to ensure it complies with federal guidelines and laws.

# 4.0 Critical Assets, Applications, and Resources

## 4.1 Identification

Processes must be implemented to detect assets hosted on the company’s network regularly. This will ensure that all assets are accounted for so security teams can apply the terms of this policy to them.

**Such processes would include:**

* *Host identification* – This would involve performing scans using a program such as Nmap to find hosts that exist on the network.
* *Site surveys* – This would involve surveying the site to discover what devices are on the network and the purpose of these systems (“How to perform an asset audit”, 2024).

## 4.2 Inventory

### 4.2.1 Systems

The following list contains critical systems operated by the company:

* PoS systems
* Front-facing web servers
* Front-facing application servers
* Email servers
* Data centers
* Endpoint computers
* Networking hardware—routers, access points, switches/hubs
* Internal media servers

### 4.2.2 Data

The following list contains critical data stored on the systems above:

* Trade secrets
* Employee and customer PII
* Financial information and transactions

### 4.2.3 Applications

The following list contains the applications that the company uses:

* PoS software
* In-house software solutions
* Default endpoint services—SSH, FTP, etc.
* Online financial portals

# 5.0 Risk Assessment

## 5.1 Risk analysis meetings

Security teams perform risk analysis on the company network every six months. This would require a process involving four steps.

### 5.1.1 Identify potential risks

Security teams must meet regularly to brainstorm potential risks the organization may face. This would involve analyzing multiple sources such as vulnerability scans, configurations/policies, data, systems, etc. to determine what could be affected by threats or threat actors.

### 5.1.2 Estimate impact of risks

The company must them analyze how it could be impacted if risks occur. This would include scoring the risks using a risk assessment matrix, allowing the security team to prioritize which risks should be mitigated first.

### 5.1.3 Report risks

Any risks that are discovered must then be reported, including details about the risk, its likelihood/impact, and the impact of the risk occurring. This information must be broken down into visuals, charts, and graphs to make the information easy to understand for all employees and executives who will review the report.

### 5.1.4 Devise a solution

A solution must then be developed based on the reported information as well as the priorities assigned to each risk. This would ensure an efficient response process that fixes the most pressing issues while still accounting for other risks that may impact the company.

Before enacting this plan, security teams must gain consent from executives. Throughout the process, the team members must be in constant communication and continually review progress, ensuring the process is as smooth and efficient as possible.

## 5.2 Vulnerability scanning

Regular vulnerability scans and assessments must be conducted regularly to discover any assets related to company assets. This information can then be used with data from other risk assessment methods to develop a well-rounded approach.

*See Section 6.0 for more details.*

## 5.3 Penetration testing

The company must perform regular penetration testing to discover vulnerabilities that may not be discovered during a vulnerability scan. This would allow testing to be customized for the company and the assets on the network, allowing for a more secure security solution that fits the company’s needs.

This can be done through in-house testing or testing by third-party security firms:

* **In-house testing** must ensure the tests align with the company’s information security and acceptable use policies. This would allow all activity to remain secure. Additionally, activity should follow a reputable attack model (Cyber Kill Chain, MITRE ATT&CK, etc.). During an attack, internal analysts must analyze activity to find indicators and update their security measures.
* **Third-party testing** must involve signing non-disclosure agreements between both parties to prevent vulnerabilities and other sensitive information from being disclosed. This would also require consequences for malicious activity and researching penetration testing organizations to minimize the chances of third parties abusing their privileges.

# 6.0 Ongoing Vulnerability Assessment

## 6.1 Vulnerability scans

Systems must be regularly scanned to determine vulnerabilities within the software, OS, and services. This would ensure a swift response to remediate these vulnerabilities, reducing the overall attack scope. To do this, a vulnerability assessment team must be assigned to run regular scans and report findings to senior security professionals.

**This would include the following steps:**

1. *Determine scope* – Assess which systems will fall under the scope of the assessment. This would include IP addresses, subnet masks, and credentialed vs. non-credentialed scans.
2. *Perform scan* – Enter details into a company-approved vulnerability scanner and run the scan on the systems under the scope.
3. *Review results* – The team must then review the findings to determine their risk and impact, detecting and excluding false positives in the process.
4. *Report findings* – The results must then be compiled into a risk analysis report prioritizing the vulnerabilities based on likelihood and impact.
5. *Develop plan* – Finally, a remediation plan must be developed by prioritizing vulnerabilities based on the company’s risk appetite. The steps within the plan must then be taken based on priority and time required (“What is risk analysis?”, 2022).

**The information that must be reported during the assessment includes (but is not limited to):**

* Vulnerabilities
* CVE identifiers
* Affected systems
* Affected software/operating system
* Software/operating system versions
* Port(s) involved
* Severity levels (if applicable)
* Estimated time to remediate

Assessments must be performed quarterly with prior consent from security executives. This ensures the activity is properly accounted for and measures can be taken to ensure availability during the scan. Failing to do so could prevent the assessment from being properly tracked and cause communication gaps between executives and the vulnerability assessment team.

## 6.2 Site surveys

Network teams must perform regular site surveys to detect the presence of unauthorized systems and access points on the network. This would allow the teams to remove any systems that may be used to compromise the network and respond to potential attacks they may have facilitated.

**This would involve the following process:**

1. *Plan the survey* – The team must identify which areas must be processed to ensure the process stays focused for maximum efficiency. Members must also be familiar with current infrastructure to identify unauthorized systems and hardware.
2. *Gather details* – Details about systems found should be collected during the survey. This would include:
   1. Building/floor
   2. Area located
   3. Name of system/access point
   4. SSID (if applicable)
   5. Signal strength (if applicable)
   6. Additional information
3. *Report findings* – After completing the survey, team members must report their findings to the networking team to ensure swift action can be taken against systems that should not be present (“Why is a wireless site survey needed?”, 2022).

## 6.3 Phishing simulations

Security executives must launch regular phishing simulations to assess human vulnerabilities in their workforce. These simulations would be sent to all employees every six months to detect if any employees could facilitate a real phishing scenario. If employees respond unfavorably, the security team must respond by providing online training, ensuring they can detect factors that may signify social engineering.

## 6.4 Code analysis

Software programs developed in-house must be regularly tested and analyzed to minimize the number of security flaws within the code. This would prevent the unintended exposure of user data or other critical information.

**To do so, the following steps must be taken:**

1. *Dynamic analysis* – This would ensure that the program runs as expected, finding most vulnerabilities upfront and shortening the analysis process.
2. *Fuzzing* – This would ensure user input is properly validated, preventing injection-based attacks that could allow PII, login credentials, or session information to be exposed or otherwise compromised.
3. *Static analysis* – This would ensure that programmers detect any vulnerabilities that the previous tests may have missed, confirming that the program is free of any noticeable issues.
4. *Repeat tests* – All tests must be repeated to ensure all vulnerabilities have been found and remediated. This should be done until all tests return no vulnerabilities (“Secure coding practices”, n.d.).

Programs should be analyzed before each public release, ensuring that they are made public in a secure form.

# 7.0 Risk Reduction

## 7.1 Gap analysis

Regular gap analysis must be performed to ensure that systems, policies, and configurations meet secure guidelines. Doing so would reduce risks and increase compliance with regulatory laws and frameworks.

**This would involve the following process:**

1. Define the state that the company wants to reach.
2. Assess the current state of the network and configurations.
3. Compare the differences between both states.
4. Report the differences between the states and prioritize gaps.
5. Develop a plan to reach the desired state (Weller, 2018).

## 7.2 Patch management

Software and operating systems must be regularly patched to ensure computing systems are properly safeguarded against known and zero-day vulnerabilities. This would reduce the attack surface by limiting the number of vulnerabilities within each of the systems. To ensure that systems are properly safeguarded, patches must be checked every week and updated accordingly by submitting a patch request. This would allow all updates to be properly tracked while keeping systems and software as secure as possible.

## 7.3 System upgrades

Operating systems must be regularly upgraded to new major versions to reduce the number of vulnerabilities while minimizing the use of legacy software. This would involve analyzing the hardware requirements of each new version and upgrading physical systems when necessary, ensuring the new systems can support the latest OS versions.

## 7.4 Platform diversity

Multiple platforms and operating systems must be used through the company network to limit the scope of an attack. Because each system would have its own unique vulnerabilities, attacks would only be limited to the ones that have common vulnerabilities. For example, while some servers may run on Ubuntu, others must run on Windows Server to prevent Linux-targeted attacks from affecting Windows systems.

# 8.0 Incident Response Planning

## 8.1 Preparation

The company must implement controls to prevent attacks and detect potential indicators of a security incident. This would involve a variety of measures to provide a layered defense system:

### 8.1.1 Backup systems

If cyberattacks compromise critical data or systems, backups should be kept to ensure they can be efficiently restored. This, in turn, will minimize downtime while mitigating the effects of a data breach. Clean backups will allow systems to be restored without malware or changed configurations.

To accomplish these, the company must implement weekly incremental backups. These backups must be stored in a 3-2-1 format where three backups are stored, two of which are stored on one system and one off-site. This will ensure a backup is always available, even if attackers corrupt ones stored in one location.

### 8.1.2 Configuring SIEM tools and log aggregation

All network activity must be logged and aggregated in a central source. This data would be sent to SIEM software configured within the SOC team for analysis. Doing so would ensure that attack indicators can be detected, allowing the incident response team to act as quickly as possible.

To do this, sensors and mirror ports must be configured on all systems throughout the network. These sources would forward data to the SIEM software, which would de-duplicate data for a more accurate analysis. Once an attack is detected through these aggregated logs, the SOC team would escalate the issue to the incident response team for analysis and eradication.

### 8.1.3 Implement technical controls

Hardware and software controls must be implemented to manage security throughout the network. This would provide a layered security approach by allowing multiple controls to be placed in various areas of the network as well as implement host-based solutions as a final “catch-all.”

**Doing this would require the following controls to be implemented:**

* Next-generation firewalls
* NIDS/NIPS
* HIDS/HIPS
* DMZ
* Antimalware

### 8.1.4 Segment networks

Across the States Bank’s network must be logically segmented to contain potential cyberattacks that may occur. This would reduce the overall scope of these attacks since attackers could not break out of the subnet they accessed. To ensure maximum security, the network must be micro-segmented, placing only two or three systems maximum within each subnet. This would minimize the effects of the incident and reduce the amount of data the attacker is able to gather and exfiltrate.

### 8.1.5 Train employees

Security teams and employees must be provided regular training sessions to ensure they can properly detect and respond to security incidents. This would include:

* Tabletop exercises
* Online training
* Phishing campaigns
* Simulated incident response

Simulations and tabletop exercises must be completed every six months to ensure they are always aware of current best practices. This also allows the company to update the incident response plan, ensuring an effective response during a real-world attack.

## 8.2 Detection & analysis

### 8.2.1 Continuous analysis

SOC teams must analyze logs generated from endpoints and networking devices to detect signs of potential cyberattacks. These logs should be sent to SIEM tools for aggregated analysis and notifications. This will ensure that SOC analysts have the necessary details to escalate the issue.

### 8.2.2 Escalation

If an attack is detected, it must be escalated to the CSIRT’s first responders for further analysis. Once an attack has been discovered, it must be escalated to the Digital Forensics Team while the CSIRT contains and eradicates the threat. This would ensure an efficient response where all team members perform individual, focused duties.

## 8.3 Containment

### 8.3.1 Short-term

Immediate steps must be taken during a cyber incident to contain the attack as soon as possible. These steps would provide initial containment before longer-term strategies can be implemented later in the process.

**Some short-term strategies may include:**

* Disconnecting affected systems
* Air-gapping subnets impacted by the attack
* Disconnecting routers to prevent malicious traffic from spreading

Ultimately, the attackers should not be aware that the security team is responding. This would allow the security team to analyze the attacker’s activity to better understand his TTPs and motivations.

### 8.3.2 Forensics

After the attack has been contained, the forensics teams must create a digital image of the affected systems to analyze the effects of the attack. This would allow the security teams to understand what the attacker was doing and how they attempted to achieve their objectives.

### 8.3.3. Long-term

Once forensic images have been taken, the CSIRT must implement longer-term solutions for containing the attack to ensure attackers cannot perform greater damage to the systems.

**Some long-term strategies may include:**

* Patching system vulnerabilities
* Removing backdoors
* Re-routing traffic to alternate subnets

## 8.4 Eradication

### 8.4.1 Disable systems

Any systems that were compromised during the attack must be immediately powered down. This would break any sessions from the attacker’s machine, ensuring the attack cannot continue.

### 8.4.2 Scan systems

While systems are disconnected from the network, they must be scanned for malware and vulnerabilities that may have been used to facilitate an attack. Doing so would allow the CSIRT to gain information about how the attackers were able to gain access outside of the company’s security. Additionally, any malware that may have compromised systems and data would be detected so it can be eradicated.

### 8.4.3 Mitigate vulnerabilities

Once vulnerabilities have been discovered during the scans, the security team must mitigate them as much as possible by removing malware, installing security patches, and implementing similar security controls to prevent the attacker from continuing or restarting an attack once the network is operational.

## 8.5 Recovery

### 8.5.1 Apply backups

System backups must be restored to restore operations. This would ensure the removal of malware and restore data that may have been compromised by the attack. To ensure a safe backup procedure, the backups must be sanitary, preventing malware from being reinstalled after the process.

### 8.5.2 Check configurations

In case attackers may have changed any configurations and registry to facilitate the attack, these settings must be reviewed after a threat has been eradicated. This would ensure that all security baselines are met and any unauthorized changes can be remediated as soon as possible, preventing misconfigurations from being exploited again in the future.

### 8.5.3 Continue monitoring

After the systems have been recovered, the security analysts must continue to monitor affected systems to ensure that the threat has been completely eradicated. This would ensure that the CSIRT can respond if the attacker still has access to the company network.

## 8.6 Post-incident activity

### 8.6.1 Reporting

Once systems have been recovered and the attack has been fully eradicated, details of the incident response process and the attack itself must be thoroughly logged and reported. These details would then be used later to analyze the attack and determine ways the incident response process can be improved and updated.

**Reports should contain the following details:**

* Systems affected
* Details left by the attacker
* Teams involved (and their members)
* Root cause
* Timeline of the attack
* Timeline of the response
* Initial response
* How the attack was eradicated
* Steps taken to recover systems

### 8.6.2 Meeting

The CISO must organize a post-incident meeting with the various security teams involved to discuss the attack and the steps that were taken to mitigate it. All team members must contribute by discussing their experiences, asking and answering questions about the incident, and finding ways to improve the steps taken.

**The following talking points must be included in each meeting:**

* The attacker(s)
* The threat vector(s)
* The cause of the attack
* How the attack was discovered
* What assets were targeted
* The attacker’s motivations
* What steps were taken during the incident response process
* How each step could have been done better

### 8.6.3 Changes

Once the meeting is over, the security teams must outline a plan that would implement the changes discussed. This would ensure an efficient response to the attack by securing the network against similar threats as soon as possible while updating the incident response plan to enable a swifter, more effective response to such events.

# 9.0 Business Continuity & Recovery

## 9.1 Business Continuity

### 9.1.1 Reroute traffic

After an attack has been contained, network traffic must be rerouted in a way that does not interact with the affected segment. This ensures that network devices can still communicate without relying on compromised parts of the network. If possible, traffic that is sent to the affected part must be rerouted to an alternate, redundant segment that accomplishes the same purpose, ensuring operations involving impacted systems can continue until the original systems are restored.

### 9.1.2 Implement physical alternatives

In case digital systems and workflows are no longer available, Across the States Bank must have alternative workflows that involve physical systems. This would ensure that the company is not fully reliant on its computing systems in case they cannot be used during a cyber incident. This would allow business operations to continue despite the lack of critical systems.

**Such physical systems might include:**

* Paper receipts instead of digital receipts
* Whiteboards and poster boards instead of digital presentations
* Paper copies of documents instead of computerized documents
* In-person meetings
* On-sites customer interactions and transactions

### 9.1.3 Configure alternate communication channels

The company must have multiple channels of communication open to ensure teams are always able to communicate with each other. This would everyone can still contact each other if the main method of communication is not available.

**This would include the following methods:**

* SMS
* Email
* Instant messaging platforms
* In-person communication
* Video conferencing platforms
* Paper-based communication

## 9.2 Business Recovery

### 9.3.1 Prioritize critical systems

If there are certain systems that the company especially relies on, the CSIRT must prioritize these systems first to ensure that critical operations can be restored as quickly as possible. This would be done by running heuristic malware and vulnerability analysis and eradicating any malware that may be present. If possible, the systems must be restored from clean backups that are stored on-site in offline data centers. This would provide the most efficient form of recovery possible by allowing easy accessibility to the backups.

### 9.3.2 Restore from backups

Affected systems must be restored from backups as quickly as possible to remove any files or vulnerabilities that might facilitate the cyber incident. Backups of critical systems must be stored in a 3-2-1 format, where two backups are stored on-site and one is stored off-site. This would ensure they can be accessed quickly while having an extra backup stored elsewhere in case on-site backups are corrupted. All systems must be backed up using an incremental system, allowing for the greatest level of efficiency.

### 9.3.3 Reset credentials

If certain accounts have indicators of a password attack, the security teams must respond by working with the IT and IAM departments to change credentials for impacted systems and services. This would ensure that any credentials attackers might have accessed will be rendered useless.

To do this, company-wide password reset mandates must be pushed out, requiring users to change their passwords the next time they log in. This would ensure that everyone changes their credentials and that their current credentials are not usable by bad actors.

### 9.4.4 Review response

The CISO must follow up every incident with a post-incident meeting to discuss the attack and the results of the process. Doing so would help the company secure its networks to prevent similar attacks in the future while updating the incident response process to increase efficiency and effectiveness.

# 10. Conclusion

This document is designed to provide maximum security for Across the States Bank’s data and systems through risk management, vulnerability mitigation, incident response, continuity of operations, and incident recovery. This will ensure greater network visibility, more efficient responses to cyber incidents, and a greatly reduced attack surface, ensuring the effects of an attack are minimized as much as possible.

* The SOC, CSIRT, digital forensics team, and security executives must be involved to contribute their expertise in the event of a cyberattack.
* Across the States Bank hosts several types of critical systems, applications, and data—including front-end servers, online portals, and employee/customer PII. Asset discovery processes must be conducted regularly using network scans and site surveys.
* To allow the company to discover risks, security teams must conduct regular risk analysis procedures, vulnerability scans, and penetration tests.
* Processes must be in place to discover and mitigate vulnerabilities within the company, including vulnerability scans, code reviews, and phishing simulations.
* Risks should be reduced using regular gap analysis, patch management, hardware upgrades, and platform diversity.
* Should an incident occur, Across the States Bank must have a thorough incident response process that allows for quick and efficient responses at each step. Each team must work together by accomplishing their specialized purposes at various points throughout the process.
* During an incident, steps must be taken to ensure that business operations continue, including rerouting traffic, using alternative methods without computers, and using alternate channels for communication.
* Business operations should be restored as quickly as possible to ensure minimum downtime. This will be done by restoring critical systems first, applying backups to affected systems, mandating that users change credentials for impacted services, and updating the incident response plan for a more efficient procedure in the future.

# 11. References

How to perform an asset audit. (2024). *Sortly*. Retrieved July 12, 2024 from https://www.sortly.com/blog/how-to-perform-an-asset-audit/

Secure coding practices every developer should know. (n.d.). *Snyk*. Retrieved July 13, 2024 from https://snyk.io/learn/secure-coding-practices/

Weller, J. (2018). *The complete guide to gap analysis*. Smartsheet. Retrieved July 13, 2024 from https://www.smartsheet.com/gap-analysis-method-examples.

What is risk analysis? 6 steps to determine a project’s risk. (2022). *Indeed*. Retrieved July 12, 2024 from https://www.indeed.com/career-advice/career-development/how-to-perform-a-risk-analysis

Why is a wireless site survey needed? How does it help? (2022). *AccessAgility*. Retrieved July 12, 2024 from https://www.accessagility.com/blog/why-is-a-wireless-site-survey-needed-how-does-it-help