

**Table of Contents**

[1. Test Scope 3](#_Toc162728025)

[1.1. Background of the Organization 3](#_Toc162728026)

[1.1.1. Overview of the Organization: 3](#_Toc162728027)

[1.1.2. Excellence in Operational Management 3](#_Toc162728028)

[1.1.3. Compliance with Regulations: 3](#_Toc162728029)

[1.2. Scope Development 3](#_Toc162728030)

[1.2.1. Interviews and Questionnaires 4](#_Toc162728031)

[1.2.2. In–scope 4](#_Toc162728032)

[2. Rules of engagement 5](#_Toc162728033)

[2.1. Rules and regulations 5](#_Toc162728034)

[2.2. Ethical Guidelines 5](#_Toc162728035)

[3. Executive summary 5](#_Toc162728036)

[3.1. Business Risk identification 6](#_Toc162728037)

[4. Vulnerability Report 8](#_Toc162728038)

[4.1. Introduction 8](#_Toc162728039)

[4.2. Target Information Gathering 8](#_Toc162728040)

[4.2.1. Reconnaissance 8](#_Toc162728041)

[4.2.2. Vulnerability Identification 11](#_Toc162728042)

[4.2.3. Solutions for above physical security issues 11](#_Toc162728043)

[4.3. Management security 13](#_Toc162728044)

[4.3.1. Weak Access Controls: 13](#_Toc162728045)

[4.3.2. Unpatched Software and Systems: 14](#_Toc162728046)

[4.3.3. Lack of Security Awareness: 14](#_Toc162728047)

[4.3.4. Physical Security Risks: 15](#_Toc162728048)

[4.3.5. Insider threats: 15](#_Toc162728049)

[4.3.6. Insecure Network Infrastructure: 15](#_Toc162728050)

[4.3.7. Data Breaches: 16](#_Toc162728051)

[4.3.8. Compliance and Regulatory Issues: 16](#_Toc162728052)

[4.4. Operational security 16](#_Toc162728053)

[4.4.1. Operational security Evaluation 16](#_Toc162728054)

[4.4.2. Authentication and Access Control: 19](#_Toc162728055)

[4.4.3. Data Encryption: 19](#_Toc162728056)

[4.4.4. Data Privacy and Compliance: 20](#_Toc162728057)

[4.4.5. Difficulty in Tracking Changes: 20](#_Toc162728058)

[4.4.6. Increased Risk of Insider Threats: 20](#_Toc162728059)

[4.4.7. Inadequate Incident Response Capability: 20](#_Toc162728060)

[4.4.8. Compliance and Accountability Issues: 21](#_Toc162728061)

[4.4.9. User Education and Awareness: 21](#_Toc162728062)

[5. References 22](#_Toc162728063)

**LIST OF TABLES**

[Table 3.1:1: Detected Business Risk 6](#_Toc162728064)

**LIST OF FIGURES**

[Figure 3.1:1: Pie Chart for Access Control 7](file:///D:\G%2001%20-%20WD%2018%20.docx#_Toc162728065)

[Figure 3.1:2: Pie chart for Vulnerability Severity Levels 7](#_Toc162728066)

[Figure 4.2:1: Security camera footages. 9](file:///D:\G%2001%20-%20WD%2018%20.docx#_Toc162728067)

[Figure 4.2:2: Alarm system 9](file:///D:\G%2001%20-%20WD%2018%20.docx#_Toc162728068)

[Figure 4.2:3: CCTV cameras in the Office 10](file:///D:\G%2001%20-%20WD%2018%20.docx#_Toc162728069)

[Figure 4.2:4: CCTV camera pictures 10](file:///D:\G%2001%20-%20WD%2018%20.docx#_Toc162728070)

[Figure 4.2:5: Main Entrance to the Office 12](file:///D:\G%2001%20-%20WD%2018%20.docx#_Toc162728071)

[Figure 4.2:6: Record Room 12](file:///D:\G%2001%20-%20WD%2018%20.docx#_Toc162728072)

[Figure 4.2:7: Some Files store on a rack 13](file:///D:\G%2001%20-%20WD%2018%20.docx#_Toc162728073)

[Figure 4.4:1: Error Page 17](#_Toc162728074)

[Figure 4.4:2: Login page 17](#_Toc162728075)

[Figure 4.4:3: User Interface 1 18](#_Toc162728076)

[Figure 4.4:4: User Interface 2 18](#_Toc162728077)

[Figure 4.4:5: User Interface 3 19](file:///D:\G%2001%20-%20WD%2018%20.docx#_Toc162728078)

[Figure 4.4:6: User Interface 3 19](file:///D:\G%2001%20-%20WD%2018%20.docx#_Toc162728079)

# 

**Acronyms**

**Acronym Definition**

SQLi SQL Injection

XSS Cross-Site Scripting

WAF Web Application Firewall

CSP Content Security Policy

CSRF Cross-Site Request Forgery

Nmap Network Mapper

Dos Denial of service

DDos Distribution Denial of Service

**Abbreviation**

Ensuring the security of an online platform in this digital era, such as the Akmeemana Regional Security Division website, stands out as one of the most pressing issues. As the magnitude and complexity of cyber menace increased with time, the level of threat necessitated personnel to strive to promote the website’s integrity, confidentiality, and availability of confidential operational data and the website’s overall integrity and operation. The purpose of this report is to evaluate the security of the Akmeemana Division website. Based on our extensive test and analysis, we can present the potential vulnerabilities of the website infrastructure and security system and the operations code and network framework. Additionally, the recommendations to be implemented and resolved to make this problem more efficient are included. Since technology is growing at an unprecedented rate, so are cyber threats**.**

While the website of the Akmeemana Division acquires great significance as a portal to obtain security-related materials and information, it is still susceptible to threats and vulnerabilities. This report explores the possible risks that can compromise the efficiency and effectiveness of the website and provides a mitigation plan to address them. If the proposed recommendations are implemented, the Akmeemana Regional Security Division may improve the level of security and reliably use the website for distributing priority security materials to the public. In the time of modern cybersecurity, this study is relevant to protect the website and to demonstrate trust tothe website’s users and other stakeholders.

# Test Scope

## Background of the Organization

### Overview of the Organization:

Among the 22 Regional Secretariat Divisions in Galle District, the Akmeemana Regional Secretariat Division is located close to Galle City. Akmeemana Regional Secretariat is located between 800 - 13' and 800 - 24 East Longitude and 060 - 01 and 060 - 07 North Latitude. It is bordered by the Baddegama Regional Secretariat Division to the north, Yakkalamulla Regional Secretariat Division to the northeast, Habaraduwa Regional Secretariat Division to the east, Galle Kadawas Satara Regional Secretariat Division to the west and southwest, and Bopeda Poddala Regional Secretariat Division to the northwest.

Akmeemana Regional Secretariat Division belongs to the Akmeemana Electoral Division. This Regional Secretariat Division covers 6437 hectares. 64 square kilometres. Administratively, it consists of 63 Grama Niladhari Divisions, and it includes about 159 villages. 4% of the total land area of Galle district. It is noted for its dedication and efforts towards the development of the goodwill of the Akmeemana province. Being a government office, the Akmeemana Regional Secretariat division fulfilled its duty to the core by providing the people under the region with the utmost care by closely examining the difficulties and problems faced by its people.

Some of the responsibilities that are being fulfilled by the Akmeemana Regional Secretariat Division are Garbage disposal, Garbage transportation, Issuance of certificates of conformity, Approval of building plans, Approval of plots of land, Excavation of roads for pipe laying, Issuance of Environmental Protection Permit, Rental of playgrounds and halls, Crematory and Cemetery Service, Lighting of streets, public places, Removal of trees threatening property and personal safety, Repairing dilapidated roads. The above-mentioned Duties are fulfilled by the Regional Office and the prior duty is to provide solutions to its people.

### Excellence in Operational Management

Akmeemana Regional Secretariat Division, having a long history of serving the people of Akmeemana region, has been maintaining the highest standard in serving its people. The regional office stores valuable documents related to their people, the region, and the work. Akmeemana Regional Secretariat Division provides a great customer experience, distinguished by its experienced and friendly employees who help the people through the problems and difficulties that they face in their mundane lives, in addition to its impressive work order that they have planned and are willing to execute for better fame.

### Compliance with Regulations:

Akmeemana Regional Secretariat Division places significant emphasis on following regulatory regulations and keeping a spotless reputation. The store strictly adheres to the policies brought down by the Government of Sri Lanka and federal rules, assuring the highest degree of ethical and legal conduct.

## Scope Development

Our security evaluation for the Akmeemana Regional Secretariat Division is built on a thorough and specific understanding of its operational environment. To do this, we began our scope creation process with a series of in-depth interviews and detailed surveys administered to Akmeemana Regional Secretariat Division Employees, including the Akmeemana Regional Secretariat Division secretary and staff. These interactions provided us with essential knowledge of the Akmeemana Regional Secretariat Division's daily operations, security practices, and the specific issues that they face in their everyday work field. We were able to precisely define the scope of our investigation by encouraging open communication and knowledge exchange, ensuring that every important aspect of Akmeemana Regional Secretariat Division’s safety measures was evaluated.

Through our development efforts, we have uncovered a comprehensive organization of the Akmeemana Regional Secretariat Division’s activities. This includes their physical security measures, inventory management methods, customer data handling practices, and financial record-keeping systems dating back to the year 2000. With these insights, we can clearly distinguish the parts of our security evaluation that fall within our scope and those that do not.

### Interviews and Questionnaires

Before conducting our security assessment for the Akmeemana Regional Secretariat Division, we need to establish the boundaries and guidelines for our examination. This is a crucial phase of the process. To gather a comprehensive understanding of the organization's security measures, we interviewed important individuals such as the Employees, Security Forces, and the regional office secretary. Their input will help us determine the necessary steps for improving the Akmeemana Regional Secretariat Division's security posture.

We gathered details about the Regional Office security procedures, difficulties, and current security measures through these interviews. We collected information on access control methods, inventory management methods, training for staff, and incident response strategies. In addition, we acquired useful information regarding the Regional Office's internet presence, if it had one, to analyze any online risks. These talks provided a critical basis for our assessment, assisting us in distinguishing the components of our evaluation that were in-scope and out-of-scope.

The information gathered from these interviews and questionnaires will be critical in adapting our security evaluation to for Akmeemana Regional Secretariat Division’s particular needs and concerns. We guarantee that our review corresponds with the Akmeemana Regional Secretariat Division’s particular business procedures while thoroughly addressing possible risks by working directly with its Employees.

### In–scope

We carefully studied important aspects of the organization's security structure, extending physical and digital domains, as part of our complete security assessment customized for the Akmeemana Regional Secretariat Division. Our assessment strategy focuses on protecting the organization's valuable assets, preserving sensitive customer data, and assuring the smooth running of business activities. The following are the important aspects and components that fall within the scope of our evaluation.

**1.2.3 Out of Scope**

The ensuing rudiments are explicitly outside the disquisition parameters for the Akmeemana Division website client Data The security of client data, including particular information, fiscal details, and sale history, isn't within the compass of this assessment. programs and Procedures Being security programs and procedures applicable to the Akmeemana Division website are reviewed for compliance and effectiveness but aren't the focus of this assessment. Third- Party Systems The security of third- party systems or services not directly controlled by the Akmeemana Regional Security Division isn't within the compass of this assessment. External trouble Landscape While external pitfalls are considered in the assessment, a detailed analysis of external trouble actors or their conditioning falls outside the compass of this report. Legal Compliance Assessing the association's compliance with specific legal regulations or assiduity norms isn't covered in this assessment of the Akmeemana Division website.

# Rules of engagement

## Rules and regulations

We must follow a set of specific rules and regulations in our association with the Akmeemana Regional Secretariat Division, which, regulates not just the security assessment procedure but also the safety and integrity of their department. Since the Akmeemana Regional Secretariat Division is a government legal office it needs to follow a set of rules and standards and a set of safety requirements to secure the privacy of its holdings and details. it works under a set of legal and safety requirements, and our evaluation must adhere to these guidelines. the General Data Protection Regulation (GDPR) for customer data protection, is one of the rules and standards that the Akmeemana Regional Secretariat Division follows. In addition to these general rules, we will work closely with Akmeemana Regional Secretariat Division’s staff and management to understand their internal security and risk management policies and processes. Access control standards, data handling processes, incident response plans, and staff training programs are examples of internal regulations. Understanding and following these principles is critical to ensure that the security assessment procedures run effectively and without interrupting the Regional Office’s day-to-day operations.

## Ethical Guidelines

In our evaluation of the Akmeemana Regional Secretariat Division, we maintain a commitment to ethical behavior. This includes respecting all parties' privacy and confidentiality, obtaining specific authorization from the Regional Director and stakeholders, and practicing responsible disclosure. We promise to utilize only authorized procedures and technologies while respecting legal and ethical bounds. Our activities will be driven by principles that prioritize the regional Department’s reputation, common peoples’ trust, and ethical data usage.

Several technological flaws have been discovered in digital spaces. Unpatched software and firmware, insufficient network security, and a lack of multi-factor authentication (MFA) are examples. For example, using out-of-date SSL/TLS protocols may expose critical data to interception. Furthermore, the lack of powerful password regulations may allow unauthorized access to important systems.

In conclusion, our evaluation highlights the crucial need for the Akmeemana Regional Secretariat Division to prioritize security measures. Akmeemana Regional Secretariat Division can strengthen its defense systems, secure its precious inventory, and preserve the security and integrity of client data by resolving the highlighted risks and shortcomings. Our suggestions, which are discussed in the following sections, provide an easy path forward for avoiding these vulnerabilities and improving Akmeemana Regional Secretariat Division ‘s security posture.

**2.3 Purpose**

The Rules of Engagement delineate the frame and guidelines that the assessment platoon must cleave to during the security vulnerability assessment of the Akmeemana Division website. These rules are established to insure a structured and ethical evaluation while minimizing any dislocation to the association's operations.

# Executive summary

During our security inspection of "The Akmeemana Regional Secretariat Division," we discovered a few weaknesses and areas of concern that require immediate addressing to strengthen the Department's overall security posture. Our evaluation has identified critical components of both physical and digital security, each of which plays a critical role in protecting the Department's precious assets. We discovered possible weaknesses in access control measures, alarm systems, and the Department’s structure from a physical security standpoint. These flaws potentially expose the store to unauthorized access and theft. Notably, the use of old-fashioned alarm systems and Outnumbered CCTV placements in the departments raises worries about the Department’s capacity to respond to security breaches efficiently. Furthermore, weaknesses in employee knowledge and training threaten the store's overall security balance.

## Business Risk identification

Our analysis of the Akmeemana Regional Secretariat Division revealed serious business concerns that require quick addressing. These dangers cover a wide range of vulnerabilities, from physical security problems to digital ones. In terms of physical security, our investigation uncovered possible flaws in access control and inventory management. The risk of unauthorized entry into the store, along with the likelihood of incorrect inventory management, compromises the integrity of the Akmeemana Regional Secretariat Division 'Documents and holdings. Furthermore, a lack of staff security awareness training raises the potential for insider threats, in which employees may unintentionally contribute to security breaches. Our study of online environments revealed weaknesses such as unencrypted data transmission and redundant software. Akmeemana Regional Secretariat Division is vulnerable to data interception since it uses unencrypted methods to send sensitive client data. Furthermore, relying on out-of-date software and equipment makes you more vulnerable to hackers. By resolving these vulnerabilities as soon as possible, the Akmeemana Regional Secretariat Division can dramatically lower the chance of data breaches while maintaining client confidence. We've summarized the detected business risks in the table below to offer a full overview:

Table 3.1:1: Detected Business Risk

|  |  |  |  |
| --- | --- | --- | --- |
| Risk Type | Specific risk | Possible Impact | Mitigation Recommendation |
| **Physical Security** | Unauthorized entry | Loss of inventory | Improves access control and the security system |
| **Physical Security** | theft | Loss of Valuable Data and Documents | Installing CCTV and security Sevillians |
| **Physical Security** | Inaccuracy in inventory | Inventory loss | Developing a strong inventory system |
| **Employee Training** | Security Awareness Gap | Data Interception | Conduct awareness and computational training for the staff |
| **Data Security** | Unencrypted Data | Data interception | Implement data Encryption |
| **Data Security** | Outdated Software | cyberattacks | Installing Regular Up-to-date software patching |

* **Graphs and Charts**

Figure 3.1:1: Pie Chart for Access Control

The levels of compliance with Akmeemana Regional Secretariat Division access control procedures are represented in this pie chart. It demonstrates that while 30% of access restrictions fall short of these regulations, 70% of them adhere to strict security standards. To protect their valuable possessions and keep their operations secure, a significant amount of their access controls must comply with security standards. This graph highlights their dedication to strong security measures while also pointing up potential areas for improvement.

Figure 3.1:2: Pie chart for Vulnerability Severity Levels

This pie chart shows the different degrees of vulnerability risks found during our security analysis. Three categories—Low Severity (32%), Medium Severity (48%), and High Severity (20%)—are used to classify vulnerabilities. Prevention activities can be prioritized using these severity levels, with an emphasis on fixing the most serious flaws to strengthen their overall security position.

# Vulnerability Report

## Introduction

The Akmeemana Regional Secretariat Division website serves as a vital platform for disseminating information, providing services, and engaging with the community it serves. As an integral component of the division's digital infrastructure, ensuring its security and integrity is paramount. This vulnerability report aims to identify and assess potential weaknesses within the website's framework, highlighting areas of concern that require immediate attention to mitigate risks effectively.

Through a comprehensive analysis of the website's architecture, codebase, and configurations, this report endeavors to provide actionable insights into vulnerabilities that could compromise the confidentiality, integrity, and availability of sensitive data and services hosted on the platform. By understanding and addressing these vulnerabilities proactively, the Akmeemana Regional Secretariat Division can enhance its cyber resilience, safeguarding its online presence against malicious threats and unauthorized access.

The following sections will outline specific vulnerabilities discovered during the assessment, accompanied by recommendations for remediation. These recommendations must be implemented promptly to fortify the website's defense and uphold the trust and security of the division's digital ecosystem.

This report is intended for the stakeholders responsible for the maintenance and security of the Akmeemana Regional Secretariat Division website, providing them with valuable insights to strengthen the website's security posture and ensure ongoing protection against evolving cyber threats.

## Target Information Gathering

It is critical to begin with detailed target data collecting to execute a full security assessment targeted to the Akmeemana Regional Secretariat Division website. This phase includes learning about the physical layout, digital infrastructure, and operational operations of the Department. The information gathered at this step is used to discover possible vulnerabilities and determine the department's overall security condition.

### Reconnaissance

* **Physical Security Evaluation**

Our team evaluated Akmeemana Regional Secretariat Division physical security methods. Access control techniques, alarm systems, security cameras, as well as an assessment of the strength and integrity of doors and windows, were all examined throughout this inspection. Additionally, we conducted interviews with technical officers, and where applicable, analyzed access records.

* **Inventory Management Systems**

We did research about their inventories, log files, data systems and some databases with their permission. We examined how inventory is maintained, including recording things through inventory books and databases. We investigated the safeguards in place to avoid inventory loss. We took photographs of how they stored their files and records in their Record rooms.

* **Customer Data Handling Practices:**

We questioned customer data handling practices, with a focus on getting construction approvals and certificates, Paying Assessment taxes, collecting garbage and giving Library facilities. Our goal is to find any gaps in the security of critical information.

* **Employee Responsibilities and Roles:**

We wanted to know about the staff members of Akmeemana Regional Secretariat Division management and their specific job roles. Then we discussed with some of them and gathered information about the steps they had taken for the security of this premises and their plans to improve it. This information assists us in identifying possible insider threats and weaknesses in employee awareness.

* **Examining Financial Records:**

We examined financial data dating up to 10 years, including cash and bank ledgers, assets, liabilities, and a record of issued cheques. This study reveals potential financial weaknesses.

A room with desks and chairs

Description automatically generatedThese are some figures of security cameras and alarm systems already they have for Physical security.

Figure 4.2:1: Security camera footages.

A white box with a black window

Description automatically generated

Figure 4.2:2: Alarm system

A collage of stairs and stairs

Description automatically generated

**A wall with a tv and a window

Description automatically generated with medium confidence**

Figure 4.2:3: CCTV cameras in the Office

Figure 4.2:4: CCTV camera pictures

### Vulnerability Identification

Despite significant investments in physical security, certain vulnerabilities persist. Here are some common weaknesses which we can identify in the Akmeemana Regional Secretariat Division.

* **Social Engineering:**

Sophisticated security systems can be bypassed through manipulation of people. Attackers may deceive employees into revealing sensitive information or granting unauthorized access. Anyone can enter the office but there are no records or details about those people.

* **Poor Installation:**

Even the best security equipment can fail if not installed correctly. Faulty camera placement, ineffective locks, or misconfigured access control systems can compromise security.

* **Inadequate Locking Practices:**

Unoccupied offices, empty desks, and front desks are vulnerable. Doors should be locked during lunch breaks, and unattended desks should be emptied to prevent theft. There should be some safe lockers to store valuable physical data and files.

* **Lack of Security Training:**

Employees need proper training to recognize security risks and respond appropriately. Because when we were questioning them, we could identify they did not pay attention to physical security and the did not have training for it.

* **Unsafe written documents**

In Akmeemana Regional Secretariat Division most of valuable documents are written documents and also there are not any backup files. So, there is a big chance to misplace or destroy those files.

### Solutions for above physical security issues

1. **Access Control:**

* **Secure Entry Points:** Limit access to authorized personnel only. Install electronic locks, key cards, or biometric systems for entry doors.
* **Visitor Management:** Implement a visitor sign-in process. Visitors should wear visible badges and be escorted within the premises.
* **Access Logs:** Maintain records of who enters and exits the office. Regularly review access logs for anomalies.

1. **Surveillance:**

* **CCTV Cameras:** Install security cameras at strategic locations (entrances, hallways, parking lots). Ensure they cover blind spots.
* **Monitoring:** Regularly review camera footage. Consider motion-activated cameras for after-hours surveillance.
* **Visible Deterrence:** Make sure cameras are visible to deter potential intruders.

1. **Perimeter Security:**

* **Fencing and Lighting:** Secure the perimeter with fences or walls. Adequate lighting discourages unauthorized access.
* **Landscaping:** Trim bushes and trees near windows to prevent hiding spots.
* **Secure Windows and Doors:** Reinforce windows and use sturdy doors with quality locks.

1. **Employee Training and Awareness:**

* **Security Protocols:** Educate employees about security policies. Teach them how to handle sensitive information and report suspicious activity.
* **Social Engineering Awareness:** Train staff to recognize phishing emails, phone scams, and unauthorized requests.
* **Emergency Procedures:** Conduct drills for fire, evacuation, and lockdown scenarios.

1. **Data Security:**

* **Secure Servers and IT Equipment:** Lock server rooms and restrict access. Encrypt sensitive data.
* **Document Shredding:** Dispose of confidential documents properly. Use cross-cut shredders.
* **Password Policies:** Enforce strong password practices for computers and accounts.

1. **Alarm Systems:**

* **Intrusion Alarms:** Install alarms that trigger when unauthorized entry occurs.

1. **Physical Layout Considerations:**

* **Sensitive Areas:** Isolate areas with valuable assets (server rooms, Record rooms, executive offices).
* **Clear Desks:** Encourage employees to keep desks locking away valuables.
* **Lockable Storage:** Provide lockers for personal belongings.

1. **Computerizing:**

* **Computerize Written document:** Because of this can protect files from physical damages.
* **Use cloud storage:** Introduce cloud computing, because of this can keep backups of data.

A yellow building with blue doors

Description automatically generatedA room with a bookcase full of files

Description automatically generated

Figure 4.2:5: Main Entrance to the Office

Figure 4.2:6: Record Room

A shelf with files on it

Description automatically generated

Figure 4.2:7: Some Files store on a rack

## Management security

Information, systems, and assets are consistently protected against theft, unauthorized access, disruption, and damage by security management. This multidisciplinary field includes the development and implementation of technologies, procedures, and policies to reduce risks and safeguard organizational assets. It includes things like making sure regulatory standards are followed, risk assessment, access control, and incident response. Sustaining an effective security posture requires constant observation and modification of security protocols in response to new threats and weaknesses. Organizations can improve their resilience to possible security breaches and lessen the effect of any security incidents by implementing proper security measures and implementing proactive initiatives.

All things considered, security management is essential to preserving the availability, confidentiality, and integrity of vital assets, and protecting the organization's operations and interests from a variety of security threats.

What potential management security problems can the Akmeemana Regional Security Division of Sri Lanka be facing?

comprehensive risk assessment, access control, and other details for a report of vulnerabilities and their detailed fixes.

### Weak Access Controls:

**Challenge:**

Poor password strength or the absence of multi-factor authentication are examples of insufficient user authentication methods. Inadequate access restrictions, which let unauthorized people use systems or sensitive data.

**Solution:**

* Use multi-factor authentication (MFA) or other robust authentication techniques for gaining access to critical systems.
* Make sure people use complex passwords and enforce frequent password changes.
* Use role-based access control (RBAC) to restrict access according to duties and roles held by employees.

### Unpatched Software and Systems:

**Challenge:**

The inability to patch and upgrade software and systems regularly exposes them to known security flaws and exploits.

**Solution:**

* Create a patch management procedure to ensure that systems and software are updated with the newest security patches regularly.
* Employ automated technologies to find vulnerabilities and rank the need for patches according to severity.
* To guarantee timely updates, put in place a system to manage and keep an eye on patching activities.

### Lack of Security Awareness:

**Challenge:**

Workers might not have received enough training to identify and handle security risks like social engineering and phishing emails.

**Solution:**

* Regularly train staff members on security awareness to inform them of common security threats and effective practices.
* To assess staff members' comprehension of identifying and reacting to phishing emails, conduct simulated phishing exercises.
* Establish clear protocols for reporting suspicious activity and encourage staff to report security incidents as soon as they occur.

### Physical Security Risks:

**Challenge:**

Inadequate physical security measures, like insufficient locks, alarms, or surveillance systems, increase the risk of equipment or sensitive data theft or unauthorized access. Insider Dangers:

**Solution:**

* Install access control systems, security cameras, and alarms to strengthen physical security measures.
* Put in place stringent access controls to sensitive spaces, including data centers or server rooms.
* Regularly inspect physical facilities for vulnerabilities in security to find and fix them.

### Insider threats:

**Challenge:**

malicious or careless acts, like data theft, sabotage, or illegal access, committed by workers or contractors.

**Solution:**

* Put least privilege principles into practice to limit authorized personnel's access to sensitive data and systems.
* Keep an eye on user activity and employ behavior analytics tools to spot unauthorized access or questionable behavior.
* Provide explicit guidelines and processes for managing confidential data and hold people accountable for breaking the rules.

### Insecure Network Infrastructure:

**Challenge:**

Weak network security measures that could be used by hackers to intercept private data include unencrypted data transmission and unprotected Wi-Fi networks.

**Solution:**

* Create secure wireless networks using WPA2 or WPA3 protocols and robust encryption.
* Segment the network to keep sensitive systems and data apart from other areas of the network.
* To monitor and manage network traffic, use firewalls, intrusion prevention systems (IPS), and intrusion detection systems (IDS).

### Data Breaches:

**Challenge:**

Inadequate data protection practices raise the possibility of data breaches and leaks, such as not using encryption or managing sensitive data improperly.

**Solution:**

* To prevent unwanted access, encrypt sensitive data while it's in transit and at rest.
* Use data loss prevention (DLP) tools to keep an eye out for and stop unauthorized transfers of private data.
* Create data retention guidelines to reduce the quantity of sensitive information kept on file and routinely delete unneeded or out-of-date information.

### Compliance and Regulatory Issues:

**Challenge:**

Infractions with applicable data protection laws, regulations, or industry standards may result in legal and financial consequences for the organization.

**Solution:**

* Keep up with the organization's applicable data protection laws, rules, and industry standards.
* Perform routine compliance audits to make sure that rules and regulations are being followed.
* Put procedures and controls in place to handle certain compliance needs, including data encryption or access controls.

## Operational security

### Operational security Evaluation

Our team evaluated the Akmeemana Regional Secretariat Division's physical security methods. Operational security evaluation is a process used to assess the effectiveness of an organization's security measures in protecting sensitive information and operations from unauthorized access or compromise.

A screenshot of a computer error

Description automatically generated

Figure 4.4:1: Error PageA screenshot of a login screen

Description automatically generated

Figure 4.4:2: Login page

A screenshot of a computer

Description automatically generated

Figure 4.4:3: User Interface 1

A screenshot of a computer

Description automatically generated

Figure 4.4:4: User Interface 2

A screenshot of a computer

Description automatically generated

Figure 4.4:5: User Interface 3

Figure 4.4:6: User Interface 3

### Authentication and Access Control:

**Challenge:**

Unauthorized access to sensitive information or functionalities due to weak authentication mechanisms or improper access controls.

**Solution:**

Implement strong authentication methods such as multi-factor authentication (MFA), enforce role-based access control (RBAC), and regularly review and update access permissions.

### Data Encryption:

**Challenge:**

Risk of data interception or unauthorized access during transmission.

**Solution:**

Use encryption protocols such as HTTPS (SSL/TLS) to encrypt data in transit and encrypt sensitive data at rest using robust encryption algorithms.

### Data Privacy and Compliance:

**Challenge:**

Violation of privacy regulations or non-compliance with legal requirements.

**Solution:**

Ensure compliance with relevant regulations (e.g., GDPR, HIPAA) by implementing privacy-by-design principles, obtaining user consent for data collection and processing, and maintaining thorough records of data handling practices.

### Difficulty in Tracking Changes:

**Challenge:**

Changes to the website or its configurations may go unnoticed, making it harder to identify potential security vulnerabilities or unauthorized modifications.

**Solution:**

Implement version control systems for website code and configurations. Require approvals and documentation for any changes made to the system and conduct regular audits to ensure compliance with change management processes.

### Increased Risk of Insider Threats:

**Challenge:**

Lack of accountability and monitoring increases the risk of insider threats, such as malicious insiders abusing their access privileges.

**Solution:**

Implement user behavior analytics to detect anomalous behavior patterns and flag suspicious activities. Conduct background checks for employees with privileged access and enforce the principle of least privilege.

### Inadequate Incident Response Capability:

**Challenge:**

Without proper logging and monitoring, incident response efforts may be delayed or ineffective, leading to prolonged exposure to security threats.

**Solution:**

Develop and regularly test an incident response plan tailored to the organization's specific needs and risks. Include procedures for incident detection, containment, eradication, and recovery. Ensure that incident response teams have access to the necessary tools and resources.

### Compliance and Accountability Issues:

**Challenge:**

Inadequate logging and administrative controls may lead to compliance violations and difficulties in demonstrating regulatory compliance.

**Solution:**

Regularly review and update security policies and procedures to align with relevant regulatory requirements. Implement mechanisms to track and report on compliance-related activities, such as access controls, data handling practices, and incident response actions.

### User Education and Awareness:

**Challenge:**

User actions lead to security breaches, such as phishing attacks.

**Solution:**

Provide regular security awareness training to employees and users, educate them about common threats like phishing and social engineering, and encourage reporting of suspicious activities.

**5. Proof of Exploit**

**5.1. General Information**

We began with an assessment of potential vulnerabilities in the method of evaluating Akmeemana Regional Secretariat Division safety position by having a thorough understanding of its physical structure and online presence. This section gives a general summary of the technical environment that is being examined, including its essential elements, technologies, and resources. Our attention spans the following areas:

1. Network Infrastructure:

Akmeemana Regional Secretariat Division maintains a network internally to support its business operations, which include inventory control, point-of-sale (POS) systems, and consumer information handling.

Configuration: For in-store operations, uses a local area network (LAN), which may be connected to third-party networks for data transfers and payment processing.

Devices: Routers, switches, and wireless access points are examples of common network devices

1. Point of Sale (POS) System: Overview:

Akmeemana Regional Secretariat Division uses a POS system to simplify consumer transactions,and their work.

Hardware: Point-of-sale systems featuring card readers, receipt printers, and barcode scanners

1. Inventory Management: Methodology:

employs tangible documentation for manual inventory management. Inventory information are organized utilizing highlighting for easy identification and are categorized by ID numbers. Maintains cash and bank ledgers going back to the year 2000, as well as a record of all checks that have been written.

Compliance: Submits financial records for annual audits to the England Revenue Department.

We are better able to investigate potential vulnerabilities inside the physical Security, management Security and operational security of the organization by developing an in-depth knowledge of these technical assets and components. The assessment of these vulnerabilities and suggestions for solutions are covered in detail in the following sections of this study.

**5.2. Evidence of Exploits**

**5.2.1. Exploit for Vulnerability 1**

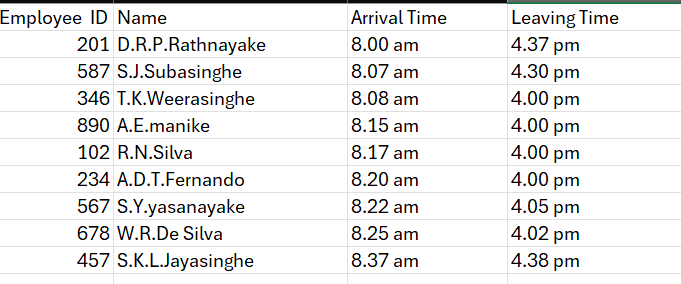
**Insider Threats:**

Because insiders have access to precious objects and may use their positions to steal, insider theft is a serious risk for Akmeemana Regional Secretariat Division. Opportunities for theft can arise from weak internal controls, such as inadequately specified or loosely executed inventory management protocols. Employee dishonesty may be made simpler by insufficient monitoring and surveillance measures, which allow them to commit crimes without worrying about being caught. Akmeemana Regional Secretariat Division should implement extensive surveillance, set strict internal controls, and thoroughly screen prospective personnel to prevent insider theft. Establishing a culture of integrity and providing regular training to employees on security procedures can also act as preventative measures and guardians against this kind of theft.

**Weak Network infrastructure:**

The Akeemana Regional Secretariat Division is at serious danger from weak network security measures, which include unencrypted data transfer and unsecured Wi-Fi networks. These vulnerabilities might lead to sensitive data being intercepted by hostile actors. Confidential information transmitted over the network, such as business correspondence, financial statements, and personal information, may be intercepted and misused if appropriate encryption measures are not in place. Furthermore, the division's lack of strong Wi-Fi security makes it open to illegal access, which gives hackers the opportunity to breach the network and compromise critical systems. It is essential that the Akeemana Regional Secretariat Division implement measures like network segmentation, firewall deployment, intrusion prevention systems (IPS), and intrusion detection systems (IDS), as well as encryption standards like WPA2 or WPA3 for wireless networks, in order to reduce these risks.

**5.2.2.1. Screenshots and Logs**

****

Insiders threat: (A Screenshot of the Employee Attendance on 4 th of April 2024 by bribing an employee of the organization)

A screenshot of a computer

Description automatically generated

Weak Network infrastructure:

**6.2.2. Exploit for Vulnerability 2**

**Wi-Fi Password Cracking:**

Attackers make use of Wi-Fi password cracking as a technique to access wireless networks. In the instance of Akmeemana Regional Secretariat Division, if an attacker learns any weak Wi-Fi passwords, they can access the network. Once inside, they might listen in on data transmissions and perhaps compromise private consumer and financial information. Attackers employ specialized software to take advantage of network weaknesses by trying popular passwords or exhaustively testing every combination. Data leaks and brand damage could result from a successful Wi-Fi password hack.

**Brute Force Attacking:**

Cybercriminals can guess weak passwords via brute force assaults, which give them unauthorized access to networks. If a hacker finds accounts in Akmeemana Regional Secretariat Division with weak passwords, they can take advantage of this weakness. To determine the best password combination, they use automated tools that test every potential combination. Once they get access to an account, they could misuse private information or carry out other assaults. A successful brute force attack against Akmeemana Regional Secretariat Division could lead to data breaches, financial losses, and reputational harm. Strong password regulations, complexity requirements, and multi-factor authentication (MFA) are crucial security precautions to take in order to avoid this.

**6.2.2.1. Screenshots and Logs**

**6.2.3. Exploit for Vulnerability 3**

**6.2.3.1. Screenshots and Logs**

**6.2.4. Exploit for Vulnerability 4**

**6.2.4.1. Screenshots and Logs**

**6.2.5. Exploit for Vulnerability 5**

**6.2.5.1. Screenshots and Logs**

**7. Remediation Report**

**7.1. Short-term Remediation Recommendations**

**7.1.1. Remediation for Vulnerability 1**

* Immediate Lock and Door Upgrades
* To improve physical access control, quickly reinforce or replace weak locks and doors.
* Immediate Security Camera Installation
* Install more security cameras in order to cover blind areas and discourage possible burglars.
* Visitor Logs
* To more efficiently monitor and control visitor access, put in place a visitor record system.

**7.1.2. Remediation for Vulnerability 2**

* + - Update any network devices' firmware right away to address any known vulnerabilities (firewalls, switches, and routers).
    - Use access control lists (ACLs) to limit access to sensitive network locations.
    - Schedule frequent scans of the network to quickly detect and repair issues.
    - Educate staff members on how to spot and avoid security risks like phishing.
    - Implement intrusion detection systems (IDS) to keep an eye out for unusual activity and to
    - create warnings.

**7.1.3. Remediation for Vulnerability 3**

* + - Implement Antivirus Software: On all endpoint devices (computers, laptops, and cellphones), install reliable antivirus software. Make sure it is up to date and configured to automatically detect and remove malware.
    - Update Software: Update the operating systems, programs, and software on all endpoints on a regular basis to reduce the risk of cyberattacks and data breaches. To fix known vulnerabilities, enable automatic updates wherever possible.
    - Employee Training: Employees should get introductory security awareness training, which should emphasize the significance of security practices including staying away from dubious email attachments and links.
    - Access Control: Limit user access to necessary resources. Ensure that employees only have access to the information and systems required for their responsibilities by implementing the principle of least privilege.
    - Endpoint Encryption: To protect sensitive data, enable encryption on endpoint devices. Full-disk encryption helps protects all data on the device and encrypted communication routes can help ensure that data transferred to and from the endpoint is secure during transmission.

**7.2.4. Remediation for Vulnerability 4**

* + - Implement access controls: Implementing access controls, such as role-based access control (RBAC), can assist in restricting access to sensitive data and systems to those employees who require it in order to fulfil their job obligations. A business can considerably reduce its vulnerability to insider threats by only allowing access to those employees who need it to perform their job duties in order to maintain appropriate access levels that are in line with employees' operations, it is also necessary to constantly examine these access credentials.
    - Perform background checks: Before granting anyone access to sensitive and personal information, performing background checks on all employees, contractors, and dealers can help you see potential threats. Such investigations can be applied to confirm a person's job history and criminal past.
    - Data loss prevention: By monitoring, identification, and avoiding any unauthorized transfer or sharing of sensitive data, a DLP system can help prevent data theft or loss. In addition to Sensitive and Privileged Data protecting sensitive data, this may additionally decrease insider threats. The warning here is that DLP providers are also targeted by the attackers, which adds another level of concern.
    - Conduct security awareness training: Offering staff frequent security awareness training can help them better understand the risks associated with cybersecurity and how they can minimize them. This might decrease the possibility of accidental insider attacks, like falling for phishing. Describe the consequences and the legal actions that can be taken against them if they engage in any kind of fraud.
    - Monitor employee activity: Applying technology for monitoring to keep track on employee use of corporate devices or the network might assist in spotting unusual conduct that might be a sign of an insider threat. Monitoring may help in identifying any strange data transfers or suspicious access patterns to sensitive data and systems. To satisfy potential privacy concerns, be sure to create clear monitoring principles and guarantee compliance with local regulations.

**7.2.5. Remediation for Vulnerability 5**

**Virtual Private Networks:** Consider employing Virtual Private Networks (VPNs) to build secure communication channels, particularly when connecting to the network from a remote location. VPNs encrypt data flow between the user's device and the company's network to provide privacy.

**Data Encryption Tools:** To secure data during file transfers or data sharing, use encryption techniques. Can use a variety of software tools and services to encrypt files and folders before transmitting them.

**Legal and Regulatory Compliance:** Determine that the encryption mechanisms adhere to applicable data protection laws and industry standards. Depending on the sort of data being handled, this could include GDPR, HIPAA, or other rules.

**Regular Security Updates**: Maintain the most recent versions of all systems, software, and security protocols. Outdated systems may contain known flaws that can be exploited

**7.3. Future Network Plan**

# References

Anon., 2019. *National Institute of Standards and Technology,* NIST Publication No. 800-53.: Guidelines for Managing Operational Security.

Johnson, A. &. L. B., n.d. Enhancing Physical Security Measures in Government Offices.. *Journal of Security Management, 15(2),* pp. 45-58.

Security, U. D. o. H., 2020. *Department of Homeland Security.* [Online]   
Available at: https://www.dhs.gov/best-practices-physical-security

Smith, J., 2005. *Security Management: Principles and Practices. ABC Publishers..* s.l.:s.n.