CNET/SYS ADMIN FINAL PROJECT PHASE 1 REPORT

Course: Computer Networks and System Administration

Student: Joseph MUTANGANA

Institution: Adventist University of Central Africa (AUCA)

Lecturer: Ins. Joshua Kayonga

Date: October 16, 2025

# Foreword

Network and system administration are the key foundation in Information Technology. Having a strong background in them would improve knowledge and skills on modern infrastructures.  
  
— BIZIMANA Lambert  
IT Officer/System Administrator  
National Bank of Rwanda

# Abstract

This report presents research conducted to understand real-world practices in network and system administration. The study focused on the National Bank of Rwanda, where a system administrator provided detailed insights through a structured Google Form interview. Key areas explored include infrastructure setup, system maintenance, policy enforcement, compliance with standards, and future technological recommendations. The results bridge theoretical learning with professional IT operations, helping strengthen understanding in network and system management.

# 1. Introduction

The purpose of this project was to study how organizations design, implement, maintain, and secure their network and system infrastructures. Through this study, I aimed to learn how technical configurations, administrative controls, and security measures work together in professional environments.

The focus organization was the National Bank of Rwanda (BNR), a leading financial institution with structured IT operations. This research helps to compare academic theories with practical implementations, showing how system administrators apply best practices in real life.

# 2. Methodology

To collect data, a structured Google Form was created based on academic guidelines provided in the project instructions. The form was shared with a system administrator at the National Bank of Rwanda, who completed it fully. The form covered daily operations, infrastructure setup, group policies, and compliance practices. The participant’s consent and confidentiality were respected, and only general practices were discussed without sensitive details.

# 3. Findings

## 3.1 Daily Operations

The system administrator performs multiple daily tasks, including network health monitoring, troubleshooting, managing user accounts, data backup, software updates, and security auditing. Common challenges are handled effectively through experience and structured troubleshooting approaches.

## 3.2 Infrastructure Setup and Implementation

The organization prioritizes security, reliability, and performance when setting up new networks. Key configurations include NAT for public/private networks, redundant internet links, VLAN segmentation, VPN access for remote users, and integration of on-premise Active Directory with Microsoft 365 AD. Firewalls, servers, and switches are used as main setup tools.

## 3.3 Policy Formulation and Enforcement

BNR enforces password policies requiring minimum length, character complexity, expiration, history restriction, and multi-factor authentication. Access control is managed through Role-Based Access Control (RBAC), ensuring users have permissions according to their roles. Network segmentation is achieved using VLANs and firewall rules. Data backups are performed daily using on-site storage systems.

## 3.4 Compliance and Security

Remote employees access systems securely through VPN connections. Security audits are performed quarterly to ensure systems meet compliance and performance standards. BNR follows international and national standards such as ISO 27001, GDPR, and national IT regulations. The organization’s overall system security level is rated strong (5/5).

## 3.5 Future & Feedback

The administrator recommended adopting cloud technologies and AI operations (AIOps) for better efficiency and modernization of IT management. These technologies would enhance automation, monitoring, and incident response.

# 4. Discussion

The practices at the National Bank of Rwanda align closely with academic concepts learned in class. They demonstrate how organizations use both preventive and corrective strategies to maintain reliable and secure systems. While theory often focuses on ideal models, real-world operations combine automation with human oversight to balance performance and compliance. The organization’s adherence to ISO standards and strong security policies reflects a mature IT environment.

# 5. Conclusion & Recommendations

This project provided valuable insights into real-world network and system administration. From infrastructure setup to daily maintenance and policy enforcement, the findings show that professional environments rely on structured procedures, clear policies, and modern technologies. Continuous learning, automation adoption, and regular compliance checks are recommended for maintaining robust systems.

# 6. References

- ISO/IEC 27001 Information Security Management Standard  
- NIST IT Infrastructure and Security Guidelines  
- Microsoft 365 and Active Directory Administration Best Practices  
- AUCA Computer Networks and System Administration Course Materials

# Appendix

Appendix A: Google Form Summary  
Appendix B: Confirmation Email Template