COMPUTER NETWROKS PROJECT REPORT

**Course:** Computer Networks

**Student Name:** Joseph MUTANGANA

**Student ID:** 29061

**Lecturer:** Ins. Joshua IRADUKUNDA

**Date:** October 17, 2025

**Report title:** Final Project phase

CNET/SYS ADMIN PHASE 1 REPORT

Table of Contents

[Foreword 2](#_Toc211527545)

[Abstract 3](#_Toc211527546)

[1. Introduction 4](#_Toc211527547)

[2. Methodology 4](#_Toc211527548)

[3. Findings (Detailed explanations) 4](#_Toc211527549)

[3.1 Daily Operations 4](#_Toc211527550)

[3.2 Infrastructure Setup and Implementation 5](#_Toc211527551)

[3.3 Policy Formulation and Enforcement 5](#_Toc211527552)

[3.4 Compliance and Security 6](#_Toc211527553)

[3.5 Future & Feedback 7](#_Toc211527554)

[4. Discussion (Expanded) 8](#_Toc211527555)

[5. Conclusion & Recommendations (Expanded) 8](#_Toc211527556)

[6. References 8](#_Toc211527557)

[Appendix 8](#_Toc211527558)

# 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 infrastructure.”  
  
— BIZIMANA Lambert  
IT Officer / System Administrator  
National Bank of Rwanda

# Abstract

This expanded report documents the findings of Phase 1 of the CNET/SYS ADMIN final project. It is based on a completed survey by an IT  
Officer/System Administrator at the National Bank of Rwanda (BNR). The report explains not only what practices the organization uses,  
but also why those practices are adopted, with short explanations linking each multiple-choice selection to real-world reasons.  
The expanded explanations help readers (and examiners) understand the practical motivation behind each technical decision.

# 1. Introduction

The aim of this project is to study how professional organizations establish, maintain and secure their network and system infrastructures.  
This expanded report uses the answers provided by BIZIMANA Lambert (IT Officer / System Administrator) at the National Bank of Rwanda to  
illustrate common industry practices and the reasoning behind them. Each selection in the survey is explained to show how these choices  
support security, reliability, and operational efficiency.

# 2. Methodology

Data was collected using a structured Google Form survey sent to IT professionals. The participant from BNR completed the form. Additionally,  
the researcher performed a field visit to BNR to introduce the study and share the form link directly with staff. Responses were anonymized  
in the reporting of sensitive details, and the participant agreed to general disclosure of practices.

# 3. Findings

## 3.1 Daily Operations

Reported daily tasks (BNR - Bizimana Lambert):

- Monitoring network health  
- Troubleshooting connectivity issues  
- Managing user accounts  
- Backing up data  
- Updating system software  
- Security auditing

Explanation: These tasks reflect a standard day for a system/network administrator in a bank. Monitoring network health (using  
dashboards, SNMP, or monitoring tools) allows the team to detect issues early. Troubleshooting connectivity and managing accounts are  
operational essentials: banks must ensure users can access services and that access is correctly controlled. Daily backups indicate a  
strong data-protection posture: the respondent chose 'daily' because financial data must be recoverable quickly. Regular updates and  
security audits keep systems patched and compliant. Together, these tasks reduce downtime and protect customer data.

Participant comment on challenges: "handled challenges only" — interpreted as a proactive approach where the team resolves  
issues as they appear using playbooks, logs, and escalation paths.

## 3.2 Infrastructure Setup and Implementation

Selected priorities when building networks: Security, Cost, Reliability, Speed/Performance

Explanation: In a bank, security is the top priority because systems hold sensitive financial data. Cost is important because infrastructure  
must be sustainable; banks balance security with budget. Reliability and performance are essential so customers and staff experience  
consistent service. These priorities explain why the participant selected redundant internet links and NAT (to separate public services from  
private internal networks) and used VLANs to segment traffic.

Implemented configurations (BNR): NAT, Redundant internet links (active/standby), VLAN segmentation, VPN access, Active Directory, Microsoft 365 AD integration

Explanation: NAT is used to hide internal addresses and protect internal hosts while allowing controlled external access. Redundant  
links (active/standby) prevent total loss of internet connectivity — critical for banking operations. VLAN segmentation separates user groups  
(e.g., employees, servers, guests) to reduce attack surface and policy scope. VPN supports secure remote access for administrators or remote  
workers. Active Directory is the standard identity service in many organizations; integration with Microsoft 365 allows centralized  
identity and email management while supporting cloud-based productivity.

Tools used: Firewalls, servers, switches

Explanation: Firewalls enforce traffic rules and protect internal networks. Servers host services (DNS, AD, email, file shares). Switches provide  
network connectivity and support VLANs; these are the essential building blocks of any enterprise network. The participant choosing these  
reflects practical, hardware-oriented infrastructure management common in banks.

## 3.3 Policy Formulation and Enforcement

Password policy: minimum length, complexity, expiration, history restriction, multi-factor authentication (MFA)

Explanation: MFA and strong password policies reduce the risk of account compromise. Password history and expiration prevent reuse of old  
weak passwords. Banks typically enforce strict authentication controls to comply with regulations and reduce fraud risk.

Access control method: Role-Based Access Control (RBAC)

Explanation: RBAC simplifies permission management at scale by assigning rights based on job role rather than to individual accounts. For  
banks with many employees, RBAC reduces mistakes and ensures that staff have the least privilege required to do their jobs.

Network segmentation: Separate VLANs and firewall rules

Explanation: Segmentation isolates different types of traffic (e.g., teller systems vs guest Wi‑Fi) so a compromise in one area does not lead  
to full network compromise. VLANs plus firewalling allow fine-grained control between segments.

Backup frequency: Daily — Primary backup method: On-site storage

Explanation: Daily backups are common in financial institutions because transactions occur continuously and data recovery windows must be small.  
On-site backups give quick recovery and control over data; many banks keep local backups and may also replicate to other sites for disaster  
recovery (noted here as on-site for speed and control).

## 3.4 Compliance and Security

Remote access: VPN

Explanation: VPN provides encrypted tunnels and access control, which are necessary when administrators or authorized staff access internal  
systems from outside the corporate network. Using VPN reduces exposure compared to direct remote services.

Security audit frequency: Quarterly

Explanation: Regular (quarterly) reviews balance thoroughness and practicality. Audits check configuration, logs, patching, and compliance. In the  
banking environment, regular audits are needed for regulatory requirements and continuous improvement.

Security rating: 5/5 (Strong)

Explanation: The participant assessed their environment as strong — consistent with their use of MFA, RBAC, daily backups, VLANs, and  
regular audits. A strong rating reflects mature practices and ongoing governance.

Compliance standards: ISO 27001, GDPR, National IT standards

Explanation: ISO 27001 is a common framework for information security management; GDPR applies where personal data of EU residents is  
handled; national standards provide local legal requirements. Compliance demonstrates governance and legal alignment.

## 3.5 Future & Feedback

Suggested improvements: Cloud technology adoption and AIOps (AI for IT operations)

Explanation: Cloud adoption can improve scalability and disaster recovery, while AIOps offers improved monitoring, anomaly detection, and  
automated response — useful for large networks with high activity. The participant highlighted these as forward-looking improvements.

# 4. Discussion

The National Bank of Rwanda's practices illustrate a mature enterprise approach: a layered security model (MFA, RBAC, firewalls, VLANs), daily  
operational hygiene (backups, updates), and a documented compliance posture. In theory classes, students learn the concepts of availability,  
integrity and confidentiality (CIA triad). BNR shows how these principles are applied in combination: redundancy for availability, AD and RBAC  
for integrity and access control, and encryption (VPN/MFA) for confidentiality.

A key learning point: choices always involve trade-offs. For example, strict password/MFA policies increase security but require user support and  
education. Daily backups provide quick recovery but require storage capacity and management. The report recommends balancing these trade-offs  
with automation and clear policies.

# 5. Conclusion & Recommendations

Conclusion: The BNR example offers strong evidence that professional organizations follow structured, layered, and regulated approaches to  
network and system administration. Their practices align with industry standards and classroom theory.

Recommendations:

- Consider hybrid backup strategies with off-site replication for disaster recovery.  
- Continue enforcing MFA and RBAC while providing user training.  
- Pilot cloud services for non-sensitive workloads and use AIOps for improved monitoring.  
- Schedule more frequent automated health checks and maintain clear runbooks for incident response.

This expanded report can be used as a reference for both academic assessment and practical guidance for students entering system administration.

# 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 (BNR response included).

Appendix B: Official Confirmation Email Template (provided separately).