

CST 620 Prevention of Cyber Attack Methodologies
Project 4 – System Security Controls

Security Control Implementation Report

Prepared By: *Abbrin Hoagland*

Version 1.0

Contents

1. Introduction	3
2. Windows Local Account and Group Security Best Practices	5
3. Linux Local Account and Group Security Best Practices	7
4. Windows Local Account and Group Security Best Practices Implementation and Testing	9
5. Linux Local Account and Group Security Best Practices Implementation and Testing.....	12
6. Conclusion	15
7. References	17

1. Introduction

In the relentless pursuit of a secure digital frontier, FICBANK stands at the forefront, acknowledging the imperative to fortify its information processing systems against evolving cyber threats. As the custodian of sensitive financial data, FICBANK recognizes that the strength of its security posture lies not just in reactionary measures but in the proactive implementation of robust controls. The genesis of this commitment sits in the comprehensive review of Reports from previous contracts, a reflective exercise that underscores both the achievements and the evolving challenges in safeguarding digital assets.

The shift towards supporting identity and access management, particularly in the realms of Windows and Linux environments, emerges as a fundamental initiative. FICBANK, aware of its limitations in in-house expertise, has sought external cybersecurity professionals to navigate the elaborate landscape of account, group, role, and permission configurations. This collaboration is not merely contractual; it is a symbiotic partnership, driven by a shared commitment to enhancing proactive cybersecurity technical controls.

The scope of the contract is clear, delineated by business requirements that necessitate the identification, implementation, and testing of security controls based on industry best practices. The task at hand involves not only the meticulous execution of these controls but also the documentation of each step, forming the basis of the forthcoming Security Control Implementation Report.

The genesis of this report lies in the hands-on execution of tasks, where users – Dale, Cindy, Steve, and Jade – with distinct access requirements were created and meticulously assigned to groups in both Windows and Linux environments. The focus of this introductory section is not to

dwell on the procedural aspects but to underscore the strategic imperative of the undertaken endeavors.

As we delve into the subsequent sections of this report, the narrative will unfold across specific domains. The report is structured to explore best practices in Windows Local Account and Group Security, Linux Local Account and Group Security, and the subsequent implementation and testing phases for both environments. This structured approach aims to provide a comprehensive account of the methodology, decision-making processes, and the outcomes of our security control implementations.

Beyond the technical intricacies, the report is envisioned to encapsulate the ethos of our collaboration with FICBANK. It is not merely a documentation of actions taken; it is a narrative that articulates the dedication to fortifying FICBANK's digital resilience. Each section serves as a testament to the meticulous planning, strategic execution, and rigorous testing undertaken to ensure that the security posture not only meets but exceeds industry standards.

The journey outlined in this report is a proactive response to the dynamic threat landscape, an acknowledgment that cybersecurity is not a destination but an ongoing process of adaptation and enhancement. In the pages that follow, we will unfold the specifics of our approach, from identifying best practices to implementing controls and conducting thorough testing. This narrative is not just a reflection of tasks completed; it is a blueprint for the future, a testament to our shared commitment to safeguarding FICBANK's digital assets.

As we embark on this journey together, the onus lies on the collaboration between FICBANK and our cybersecurity professionals. The Security Control Implementation Report is not just a deliverable; it is a joint endeavor that aims to empower FICBANK with insights, strategies, and a fortified security posture that resonates with the organization's commitment to excellence.

2. Windows Local Account and Group Security Best Practices

Securing Windows environments demands a comprehensive understanding of local account and group security best practices. As FICBANK strives to fortify its information processing systems, a strategic focus on Windows security measures becomes imperative. This section delves into key best practices that lay the foundation for a robust security posture, encompassing user accounts, groups, and their associated permissions.

Before delving into the specifics, it's crucial to recognize that effective security measures begin with the creation and management of user accounts. The principle of least privilege serves as a guiding philosophy – granting users the minimum access necessary for their job functions. This approach mitigates the risk of unauthorized access and minimizes potential damage in the event of a security breach. (Mudd. 2023)

Windows Local Account Security Best Practices:

1. Unique Usernames and Strong Passwords:

- Enforce the use of unique usernames to prevent confusion and unauthorized access.
- Implement strong password policies, including complexity requirements and regular password changes, to enhance authentication security. (Microsoft)

2. Account Lockout Policies:

- Configure account lockout policies to safeguard against brute-force attacks by temporarily locking out accounts after a specified number of failed login attempts.

3. User Account Reviews:

- Regularly review user accounts to identify and deactivate those that are no longer necessary, reducing the potential attack surface. (Microsoft)

4. Disable Unnecessary Accounts:

- Deactivate or remove default accounts that may be unnecessary for operational purposes, as these can be exploited if left active.

Windows Local Group Security Best Practices:

1. Least Privilege Principle:

- Apply the principle of least privilege when assigning users to groups, ensuring that each group has the minimum necessary permissions for its intended purpose. (Microsoft)

2. Role-Based Access Control (RBAC):

- Adopt RBAC methodologies to align group memberships with specific job functions, streamlining access management and reducing the risk of privilege escalation.

3. Nested Groups:

- Limit the use of nested groups to maintain simplicity and transparency in group memberships, preventing unintended consequences in access management.

4. Regular Group Reviews:

- Conduct regular reviews of group memberships to ensure alignment with organizational roles and responsibilities, modifying memberships as needed.

In adherence to these best practices, FICBANK can establish a resilient foundation for Windows local account and group security. However, implementation is just one facet; rigorous testing and ongoing monitoring are essential to validate the effectiveness of these measures and adapt to evolving threats.

Post-Implementation and Testing:

After implementing these best practices, it is imperative to conduct thorough testing to validate the efficacy of the security controls. Periodic security audits, simulated attacks, and access reviews contribute to ongoing assessment and refinement. The documentation of these processes, along with any deviations and corrective actions, ensures transparency and compliance. (NIST 2023)

In conclusion, a holistic approach to Windows local account and group security involves not only the initial implementation of best practices but also continuous monitoring, testing, and adaptation. As we move forward, the subsequent sections will delve into the practical implementation and testing of these measures in FICBANK's unique operational context. The objective is not just to secure Windows environments but to fortify FICBANK's digital infrastructure against a dynamic threat landscape.

3. Linux Local Account and Group Security Best Practices

Ensuring the robust security of Linux environments demands a meticulous approach to local account and group security. As FICBANK navigates the intricacies of information processing systems, the spotlight turns to Linux, a crucial component in the organization's digital ecosystem. This section elucidates key best practices that form the bedrock for a resilient security posture, encompassing local user accounts, groups, and their associated permissions.

Before delving into the specific practices, it's vital to underscore the significance of user account management in Linux environments. Adopting the principle of least privilege ensures that users are granted only the minimum necessary access, mitigating the risk of unauthorized actions and minimizing potential damage in the event of a security incident. (Mudd 2023)

Linux Local Account Security Best Practices:

1. Unique Usernames and Secure Passwords:

- Enforce the use of unique usernames to enhance accountability and prevent confusion.
- Implement strong password policies, including length and complexity requirements, to fortify authentication mechanisms.

2. Account Lockout and Password Policies:

- Configure account lockout policies to thwart brute-force attacks by temporarily locking accounts after a specified number of unsuccessful login attempts.
- Enforce password policies such as expiration and history to maintain the security of user credentials.

3. User Account Reviews:

- Regularly review user accounts to identify and deactivate those that are no longer necessary, reducing the potential attack surface.

4. Disable Unused Accounts:

- Deactivate or remove default accounts that are not required for operational purposes, reducing potential vulnerabilities.

Linux Local Group Security Best Practices:

1. Principle of Least Privilege:

- Adhere to the principle of least privilege when assigning users to groups, ensuring that each group possesses only the minimum necessary permissions.

2. Role-Based Access Control (RBAC):

- Implement RBAC strategies to align group memberships with specific job functions, facilitating streamlined access management and reducing the risk of privilege escalation.

3. Regular Group Reviews:

- Conduct periodic reviews of group memberships to guarantee alignment with organizational roles and responsibilities, making adjustments as needed.

4. Avoid Excessive Nesting:

- Limit the use of nested groups to maintain transparency and simplicity in group memberships, preventing inadvertent consequences in access management.

Implementation of these best practices sets the stage for a robust Linux local account and group security framework. However, the true efficacy of these measures lies not just in their deployment but in the rigorous testing and ongoing monitoring that follows.

Post-Implementation and Testing:

After the initial implementation, the next crucial step is rigorous testing to validate the effectiveness of the security controls. Regular security audits, simulated attacks, and access reviews contribute to continuous assessment and adaptation. Documentation of these processes, along with any deviations and corrective actions, ensures a transparent and accountable approach to Linux local account and group security. (NIST 2023)

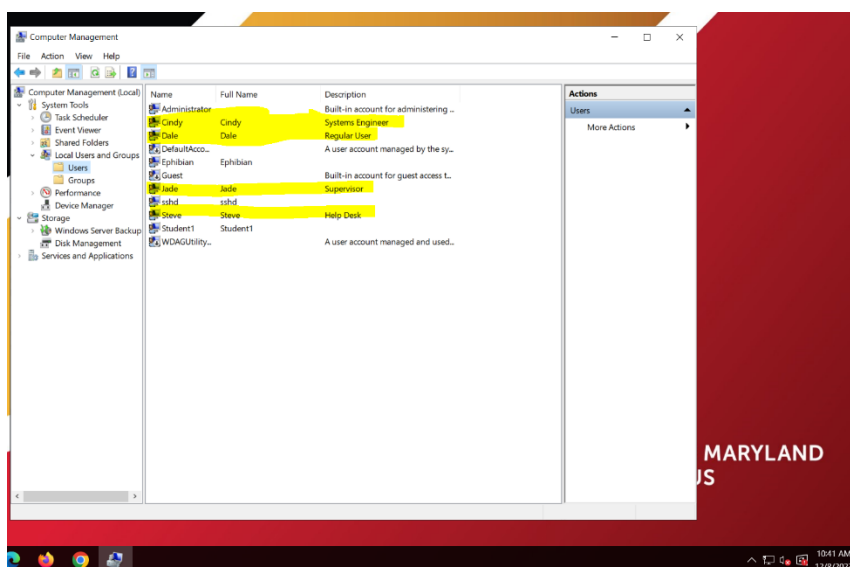
In conclusion, safeguarding Linux environments requires a holistic approach, encompassing the strategic implementation of best practices and ongoing vigilance. The subsequent sections of this report will delve into the practical application and testing of these measures within FICBANK's operational context. The goal is not only to secure Linux environments but to fortify

FICBANK's digital infrastructure against the dynamic and evolving landscape of cybersecurity threats.

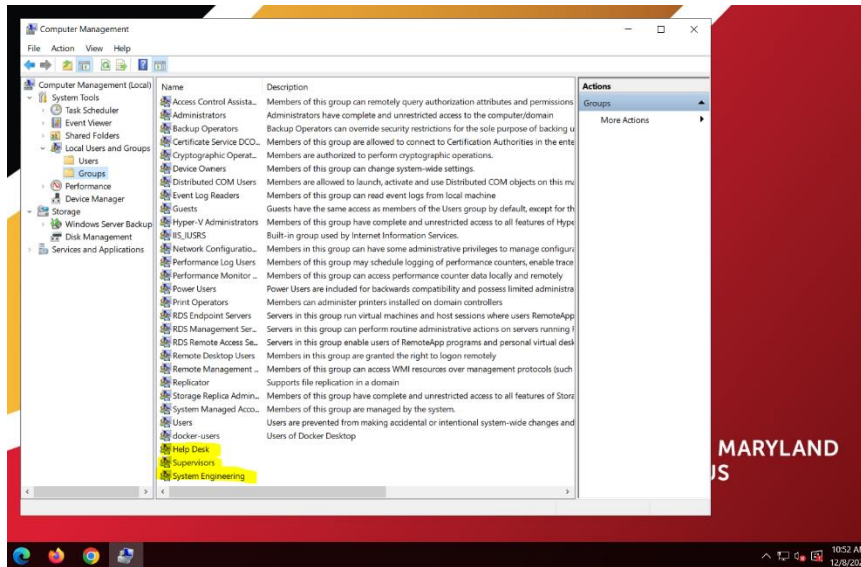
4. Windows Local Account and Group Security Best Practices Implementation and Testing

In the implementation phase of the Windows Local Account and Group Security Best Practices, our focus was on configuring user accounts and groups to align with specific job functions and subsequently testing the effectiveness of the implemented controls. This hands-on exercise unfolded within the context of FICBANK's security requirements, where four distinct users—Dale, Cindy, Steve, and Jade—were assigned roles and permissions on a Windows VM.

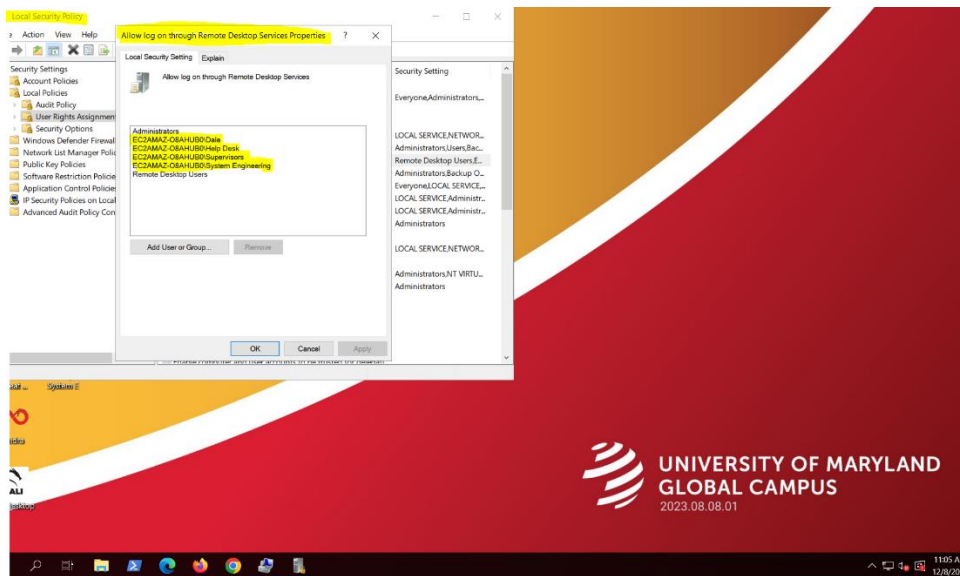
To commence the implementation, we logged onto the Windows VM and accessed the "Computer Management" tool. Within the "Local Users and Groups" section, we created user accounts for everyone, attributing descriptions based on their designated job functions. Dale, as a normal user needing remote access, Cindy as a Systems Engineer requiring unrestricted access, Steve from the Help Desk necessitating remote login capabilities, and Jade as the Systems Engineering and Help Desk supervisor.



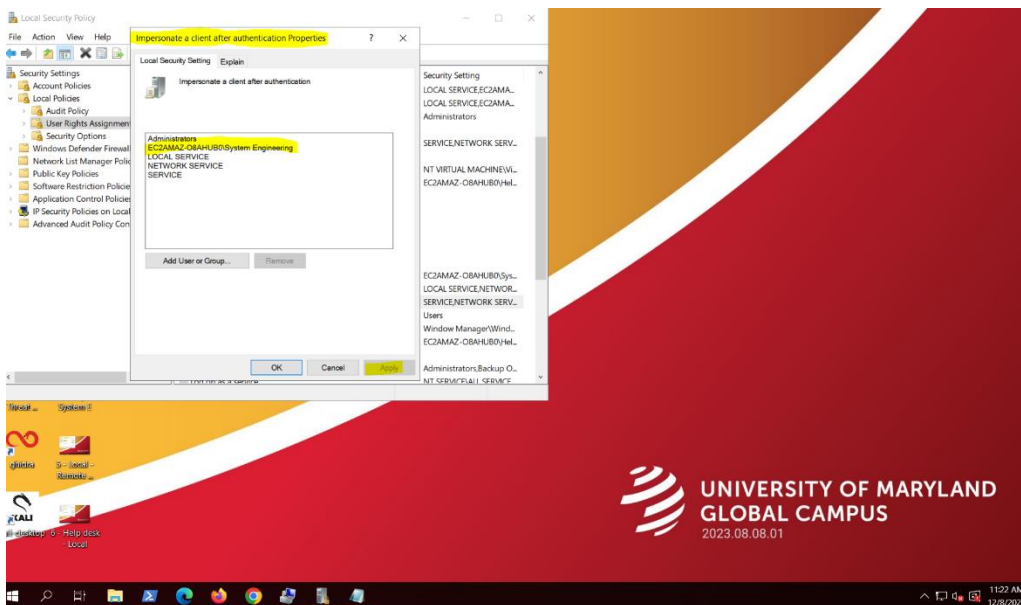
The next step involved the creation of groups corresponding to these job roles—System Engineering, Help Desk, and Supervisors. Following this, we ensured that all users were appropriately added to the default "Users" group. Each user was then assigned to their respective groups based on their job roles, establishing a foundational structure aligned with the principle of least privilege.



Moving forward, we delved into the intricacies of permissions by accessing the "Local Security Policy" through the "Administrative Tools" menu. Our objective was to grant remote login permissions by identifying the policy related to remote desktop services. Once identified, we added the relevant Ser... groups and individuals, ensuring the inclusion of both users and groups and employing the "Object Types" button for clarity.



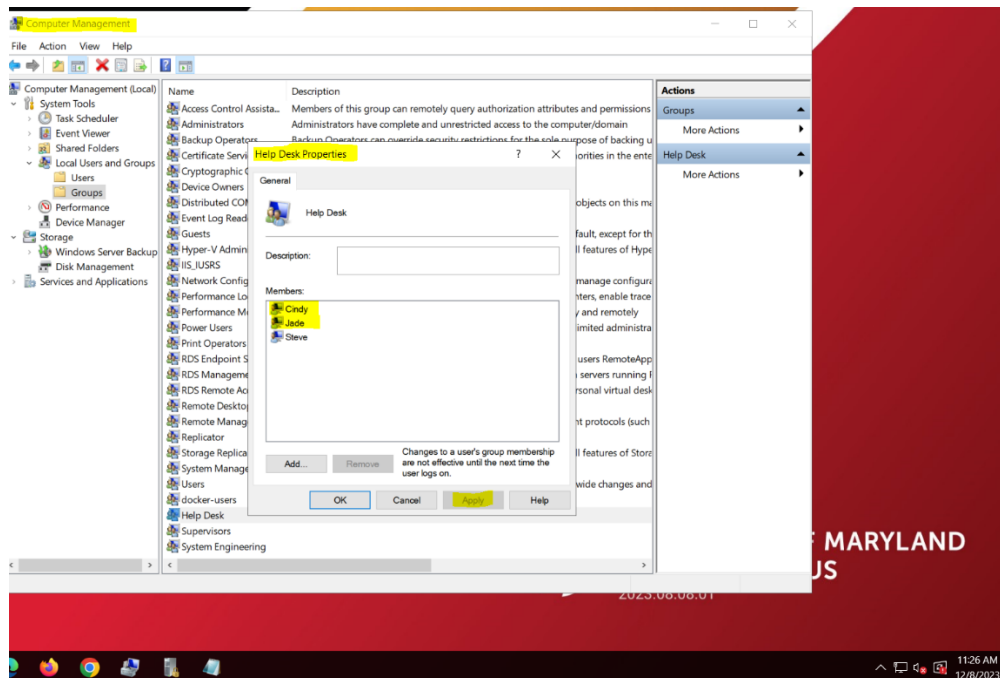
To refine access control, the focus shifted to the Help Desk group. Within the "User Rights Assignment" section, we selected "Restore files and directories" and added the Help Desk group, subsequently endowing them with specific permissions such as the ability to log on locally, access the computer from the network, and perform other specified tasks.



The final steps involved providing permissions to the System Engineering team. Instead of adding users directly to the built-in administrator group, a security-conscious approach was

adopted. Specific permissions, such as the ability to force shutdown from a remote system or manage auditing and security logs, were selectively granted to the System Engineering group.

To align the permissions of the System Engineering and Help Desk groups without duplicating access, individual users—Cindy and Jade—were added to the Help Desk group within the "Computer Management" interface.

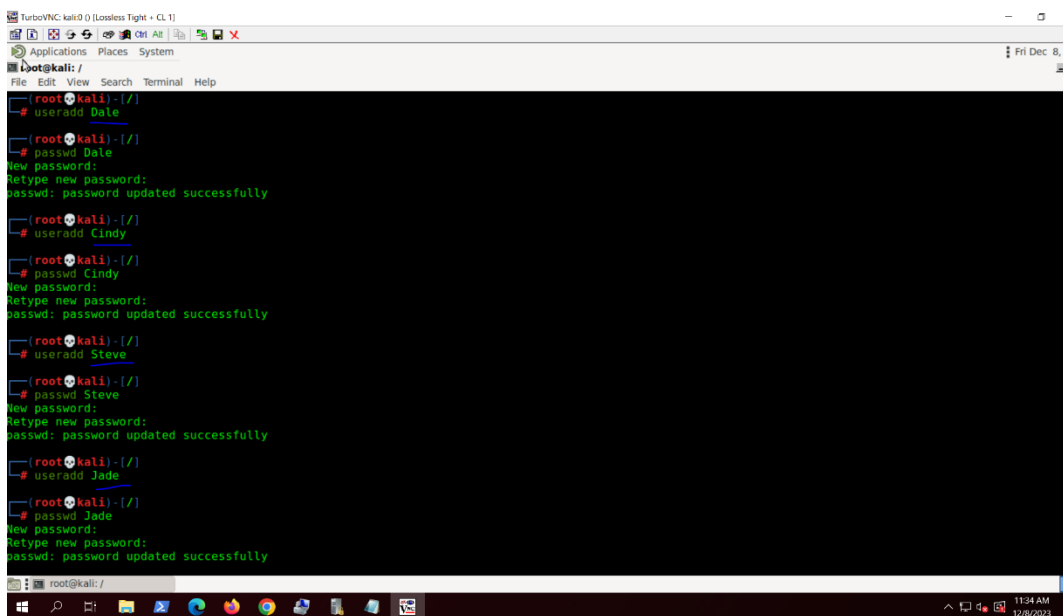


With the configurations in place, we rigorously tested the setup by logging out of the Windows VM and re-entering with the newly created users. Through this testing phase, we assessed the effectiveness of the implemented controls, noting the actions each user could and could not perform—ensuring a secure and tailored access environment reflective of FICBANK's specific security needs.

5. Linux Local Account and Group Security Best Practices Implementation and Testing

In executing the Linux Local Account and Group Security Best Practices, our focus was on practical implementation and evaluation of controls on a Kali VM, mirroring the approach taken for Windows. The objective was to align user accounts and groups with specific job functions and assess the effectiveness of the implemented security measures.

The initial step involved the creation of user accounts for Dale, Cindy, Steve, and Jade on the Kali VM. Passwords were set for each user, establishing a foundational layer for the subsequent security configurations.



```
TurboVNC: kali0 () [Lossless Tight + CL 1]
Applications Places System
root@kali: /
File Edit View Search Terminal Help
root@kali:~# useradd Dale
root@kali:~# passwd Dale
New password:
Retype new password:
passwd: password updated successfully
root@kali:~# useradd Cindy
root@kali:~# passwd Cindy
New password:
Retype new password:
passwd: password updated successfully
root@kali:~# useradd Steve
root@kali:~# passwd Steve
New password:
Retype new password:
passwd: password updated successfully
root@kali:~# useradd Jade
root@kali:~# passwd Jade
New password:
Retype new password:
passwd: password updated successfully
root@kali:~#
```

Following user creation, attention turned to configuring SSH access. The `sshd_config` file was edited from the command prompt, introducing statements for each user to permit SSH access. The SSH service was then restarted to apply these changes effectively.

```
root@kali: /  
GNU nano 3.4 /etc/ssh/sshd_config  
# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts  
#HostbasedAuthentication no  
# Change to yes if you don't trust ~/.ssh/known_hosts for  
# HostbasedAuthentication  
# IgnoreUserKnownHosts no  
# Don't read the user's ~/.rhosts and ~/.shosts files  
#IgnoreRhosts yes  
  
# To disable tunneled clear text passwords, change to no here!  
PasswordAuthentication yes  
AllowUsers Cindy Dale Jade Steve  
#PermitEmptyPasswords no  
  
# Change to yes to enable challenge-response passwords (beware issues with  
# some PAM modules and threads)  
ChallengeResponseAuthentication no  
  
# Kerberos options  
#KerberosAuthentication no  
#KerberosOrLocalPasswd yes  
#KerberosTicketCleanup yes  
#KerberosGetAFSToken no  
  
Help Write Out Where Is Cut Execute Location Undo  
Exit Read File Replace Paste Justify Go To Line Redo  
root@kali: /  
2023.08.08.01
```

To organize users based on their roles, three groups—helpdesk, systemengineering, and supervisors—were established using the groupadd command. Users were added to their respective groups through the usermod command, adhering to the principle of least privilege.

In the final stages of the Linux implementation, sudo permissions were granted to Cindy and Jade. The usermod command was employed to add these users to the sudoers group, enabling elevated permissions as required for their roles.

```
root@kali: /  
# usermod -a -G sudo Cindy  
# usermod -a -G sudo Jade  
root@kali: /  
12:02 PM  
12/8/2023
```

Verification of access and permissions was a critical aspect of the testing phase. Logging in via SSH with the designated users, Cindy and Jade, ensured that their access was aligned with the specified security parameters. The su command was utilized to elevate permissions, and the whoami command confirmed the successful transition to the root level.

Throughout this process, the emphasis was on ensuring a secure and tailored access environment reflective of FICBANK's specific security needs in the Linux domain. The implementation and testing provided insights into the effectiveness of the controls, contributing to a comprehensive understanding of the security posture within the Linux environment.

6. Conclusion

In undertaking the implementation and testing of security controls for both Windows and Linux local accounts and groups at FICBANK, our primary objective was to fortify the organization's information processing systems. The multifaceted approach included identifying, implementing, and testing best practices for identity and access management, aligning with the proactive cybersecurity technical controls goals outlined by the Board.

The Windows-focused phase involved meticulous steps to create user accounts, establish groups, and configure permissions based on the principle of least privilege. The implementation adhered to recognized best practices, ensuring a robust security foundation. Testing and evaluation of these configurations were integral, validating that the security posture was not compromised.

Similarly, the Linux environment underwent a comprehensive security transformation. User accounts were configured, SSH access was carefully managed, and groups were established to streamline permissions. The implementation embraced the security philosophy of avoiding direct additions to built-in groups, opting instead for custom groups based on distinct roles. (Red Hat)

Testing verified the effectiveness of these controls, affirming the organization's commitment to robust Linux security practices.

Throughout this endeavor, the collaboration between the cybersecurity team and FICBANK showcased a dedication to proactive security measures. The hands-on approach provided tangible insights into the practical application of security controls, emphasizing not only the technical aspects but also the strategic decision-making involved in shaping secure information processing systems.

As we submit the Security Control Implementation Report, detailing the intricacies of our work, we recognize that cybersecurity is an ongoing endeavor. The landscape evolves, threats mutate, and technologies advance. FICBANK's commitment to staying ahead of these challenges, evident in their engagement with this project, reflects a forward-looking approach to safeguarding sensitive information.

In conclusion, the successful implementation and testing of security controls for local accounts and groups on both Windows and Linux platforms mark a significant milestone in FICBANK's cybersecurity journey. The insights gained and the robust security measures put in place lay the foundation for a resilient and adaptive security posture in the face of an ever-changing threat landscape.

7. References

1. Microsoft. (n.d.). *Best practices for securing Windows local accounts and groups*. <https://learn.microsoft.com/en-us/training/modules/secure-windows-server-user-accounts/>
2. National Institute of Standards and Technology. (2023, June). *Special Publication 800-53B, Revision 6: Security and Privacy Controls for Information Systems and Organizations*. <https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final>
3. Red Hat. (n.d.). *Managing User Accounts in Red Hat Enterprise Linux*. <https://access.redhat.com/start/how-to-create-and-manage-users>
4. Mudd, G. (2023, August). *Implementing Least-Privilege Administrative Models*. <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/implementing-least-privilege-administrative-models>
5. Microsoft. (n.d.). *Restrict and protect local accounts with administrative rights*. <https://learn.microsoft.com/en-us/windows/security/identity-protection/access-control/local-accounts>