Access Control Worksheet

Notes about the User:

- The event took place on [insert date].
- The user is identified as [insert user role].
- The IP address of the computer used to log in is [insert IP address].

Event logs help identify the who, what, and why of a security incident, providing crucial details for analysis.

Access Control Issues Identified:

1. [Insert issue related to unauthorized access, e.g., "A contractor retained admin access despite their contract ending in [year]."]
2. [Insert another access control issue, e.g., "The company uses shared cloud drive access with no individual user authentication."]

Ineffective access controls can lead to security vulnerabilities, allowing unauthorized users to access sensitive data.

Recommendations for Improvement:

1. **User Account Expiration:** Implement a policy where user accounts expire after 30 days of inactivity or upon contract termination.
2. **Restricted Contractor Access:** Contractors should only have access to necessary resources, and permissions should be revoked upon contract completion.
3. **Multi-Factor Authentication (MFA):** Require MFA for all logins to enhance security.
4. **Role-Based Access Control (RBAC):** Implement RBAC to ensure that users only have permissions relevant to their role.
5. **Regular Access Reviews:** Conduct periodic audits of user access to remove outdated accounts and enforce least privilege principles.

Key Takeaways: This assessment highlights the risks associated with poor access control management, such as failing to revoke user access and using shared resources without authentication. By implementing structured authentication and authorization policies, businesses can significantly reduce security risks and prevent unauthorized access incidents.

Next Steps:

- Review and implement the recommended security measures.
- Schedule a follow-up audit in [insert timeframe] to ensure compliance with access control policies.
- Educate employees about secure authentication practices.

By taking proactive steps, businesses can strengthen their security posture and mitigate potential threats effectively.