Access Control Worksheet

Step 1: Notes from the Event Log

- The transaction originated from an unfamiliar IP address that does not match the finance manager's usual login location.
- The system log indicates that an employee account (possibly a former employee or compromised credentials) was used just before the unauthorized deposit attempt.

Step 2: Identified Access Control Issues

1. **Shared Credentials:** Employees use a shared cloud drive, which lacks proper user authentication and individual accountability.
2. **Lack of Role-Based Access Control (RBAC):** Employees have broad access to financial resources without restrictions based on job roles.
3. **Inactive Account Not Removed:** If a former employee's account was used, access was not revoked upon their departure.

Step 3: Recommendations for Mitigation

1. **Implement Individual User Accounts & MFA**
    - Require each employee to have a unique login credential rather than sharing access.
    - Enable Multi-Factor Authentication (MFA) to prevent unauthorized access.
2. **Enforce Role-Based Access Control (RBAC)**
    - Restrict access to financial transactions only to authorized personnel, such as finance managers.
    - Implement the **principle of least privilege** to ensure employees can only access what is necessary for their role.
3. **Enable Activity Logging & Alerts**
    - Set up alerts for unusual login activity, such as access from unknown locations or after work hours.
    - Maintain detailed logs and regularly review them to detect anomalies.
4. **Revoke Access for Departed Employees Immediately**
    - Implement an automated process to disable accounts when an employee leaves the company.
    - Conduct periodic audits to remove inactive accounts.

Conclusion By implementing these recommendations, the business can significantly enhance security measures, prevent unauthorized financial transactions, and ensure better accountability for employee access.