Access Control Worksheet - Completed Example

Notes (from Event Log):

- A login was recorded at 2:35 AM from an IP address not previously associated with the company network.

- The credentials used to access the system belonged to a former employee (Emily Davis), who left the company two weeks ago.

Issues (identified from comparison with Employee Directory):

- Former employee accounts are still active, allowing access to sensitive systems even after termination.

- All employees use a shared cloud drive with no individual access restrictions or logging, making it difficult to determine who did what.

Recommendations (for Mitigation):

- Implement a user deprovisioning policy that immediately revokes system access for employees who leave the company.

- Enforce role-based access controls (RBAC) and eliminate shared drive access in favor of individual accounts with permissions tailored to job responsibilities.