# Access Control Worksheet — DRAFT (Customize with your Event Log)

Use this as a ready-to-submit draft. Replace any angle-bracketed items (e.g., <DATE>) with values from your Accounting exercise (Event log + Employee directory). If you share those rows, I can generate a fully tailored version for you.

## 1) Notes about the user (add 1–2 items)

* On <DATE> at <TIME>, account <USER/EMAIL> performed <EVENT TYPE, e.g., “edited bank details”> on <FILE/FOLDER> from IP <IP ADDRESS> using <DEVICE/OS/Browser>.
* Activity occurred <during/outside> business hours and the IP <matches/does not match> an office/VPN range or expected location per the directory.

## 2) Access control issue(s) identified (list 1–2)

* Over‑permissive access on the shared cloud drive: users without a business need had edit rights to payroll data (violates least privilege).
* Weak authentication/account hygiene: no MFA and/or shared or still‑active former employee accounts; lack of a documented joiner‑mover‑leaver (JML) process.

## 3) Recommendation(s) to prevent recurrence (provide at least 2)

* Enforce SSO with MFA for all users accessing finance resources. Require unique, non‑shared identities and immediate deprovisioning at offboarding.
* Apply RBAC and least privilege on cloud storage: separate a restricted “Payroll” area, grant edit rights only to finance; others get view or no access. Require dual control (maker‑checker) for any vendor/bank changes.
* Strengthen accounting/auditing: centralize immutable audit logs, enable alerts for off‑hours access and changes to bank details, and conduct weekly reviews.
* Use conditional access: require VPN/known devices for finance apps, geofencing and impossible‑travel detection, and block risky IP ranges.
* Establish a formal JML process and quarterly access recertification for finance data; document and test the process.
* Security policy and awareness: prohibit credential sharing, require strong passwords/passphrases, and set session timeouts for sensitive apps.

## Appendix (optional to include in your submission)

AAA mapping (tie your recommendations to core principles):

* Authentication: SSO + MFA; unique accounts; device compliance.
* Authorization: RBAC; least privilege; separation of duties (maker‑checker).
* Accounting (Auditing): centralized, immutable logs; alerts on sensitive actions; periodic review.

Tip: After you confirm the actual event log details, replace the placeholders and delete any lines that don’t apply.