Project File Access Review

Example report

Kit Baroness | Security analysis example

Outcome and scope

My Linux permissions analysis reviewed a research team's project directory and identified three adjustments: remove write access from other users on a project file, make an archived file read-only for its owner and group, and restrict a drafts directory to its owner.

The source records the inspection and change procedure. The commands have also been reproduced against isolated temporary resources, with the resulting file modes retained in validation record LR-01 dated 4 November 2026. That reproduction verifies the mode changes; live-system identity, access-control-list, and service-continuity tests remain pending.

Findings and demonstrated changes

ACC-S1 to ACC-S3 refer to the supplied permission inventory and change sections. LR-01 records the isolated reproduction. Permission strings show the operating-system access settings; numeric modes provide an exact comparison.

Resource and source	Recorded before-state	Target and observed isolated result
project_k.txt / ACC-S1	-rw-rw-rw- (0666): owner, group, and others can read and write.	-rw-rw-r-- (0664): other users lose write access; owner and group retain it. LR-01: passed.
.project_x.txt / ACC-S2	-rw--w---- (0620): owner can read and write; group can write.	-r--r----- (0440): owner and group can read the archived file, with ordinary write permission removed. LR-01: passed.
drafts / ACC-S3	drwx--x--- (0710): owner has full directory access; group can traverse it.	drwx------ (0700): ordinary directory access is limited to the owner. LR-01: passed.

The first finding allows modification beyond the stated requirement. The archived-file finding combines unnecessary write permission with missing group read permission. The directory finding allows group traversal even though the requirement limits access to the owner.

The project-file target retains read access for other users because the stated rule prohibits their write access. The data owner must confirm whether that remaining read access is appropriate for the material involved.

Work performed and outstanding validation

The analysis records using ls -la to include hidden files in the inventory and chmod for the scoped adjustments. LR-01 reproduces the three mode transitions independently of a production environment.

Validation	Result	Remaining evidence
Reproduce the three mode changes.	Passed for isolated resources; observed modes 0664, 0440, and 0700.	Retain LR-01 with the review.

Validation	Result	Remaining evidence
Test required and prohibited identity access.	Not performed against the target environment.	Approved users retain necessary access; unauthorized writes and group traversal are denied.
Check additional access mechanisms and dependencies.	Not performed against the target environment.	Parent-directory permissions, group membership, access control lists, privileges, and dependent work are reviewed.

Acceptance and continuing ownership

The system administrator should capture the live before-and-after state and conduct the remaining access checks. The data owner should confirm the required read and write access before accepting the review. These roles are proposed; assignment is pending.

An archived file's ordinary read-only mode is not an immutability guarantee, and privileged access requires separate assessment. Close the review when effective access is demonstrated, dependent work still functions, and exceptions have a named owner and review date.

Reference method

The review follows access-enforcement and least-privilege concepts in NIST SP 800-53 Rev. 5, with validation structured using SP 800-53A Rev. 5.

https://doi.org/10.6028/NIST.SP.800-53r5

https://doi.org/10.6028/NIST.SP.800-53Ar5