Design Write-Up: IAM Permissions Explorer

The design solves a common IAM challenge: as cloud environments grow, permissions accumulate, creating hidden risk. Security teams need a fast, safe, and guided way to identify the riskiest users and roles and remediate excessive or unused access with confidence.

Screen 1 – IAM Permissions Explorer (Triage)

- KPI cards (High Risk Entities, Unused Permissions, Overly Broad Permissions, Admin-Level Access) provide an immediate snapshot of overall risk and help the analyst know where to begin.
- A filterable, risk-sorted list of users and roles enables a smooth transition from "overall picture" to "next entity to investigate," matching real workflows such as triaging high-severity access issues.

Screen 2 – Role Detail (Understanding & Decisions)

- A clear role header and risk gauge answer "how risky is this role overall?" at a glance.
- The permissions table (Permission, Risk, Last Used) translates raw IAM policy data into actionable insights by exposing which actions drive risk and whether they are still required.
- The "Recommended Fixes" panel converts analysis into concrete actions (remove unused, restrict overly broad, review sensitive permissions), with a single CTA to move into remediation when the user is ready.

Screen 3 – Fix Permission Flow (Confidence & Confirmation)

- Side-by-side Current Policy vs. Proposed Least-Privilege Policy, plus a concise "Changes" list, makes the before/after state explicit and auditable.
- A warning banner and short impact analysis set clear expectations that permissions will be reduced and some activity might change, building trust before applying fixes.
- The "Apply Fix" button finalizes the change only after this review, balancing security improvement with operational safety.

Prioritization rationale

- **First priority:** triage and visibility (Screen 1) so the user can quickly decide "which identity should I fix next?"
- **Second priority:** actionable understanding (Screen 2) so they can see which permissions are truly problematic and why.
- **Third priority**: safe remediation (Screen 3) to remove fear of breakage and encourage confident, repeatable cleanup.
- Advanced extras (bulk edits, rich history charts) are consciously deprioritized to keep the MVP focused on the end-to-end fix journey.

Success metrics

- **Operational**: Reduced time to remediate a high-risk role; more high-risk roles receiving at least one applied fix per week.
- **Security:** Decrease in unused and overly broad permissions; reduction in non-admin identities holding admin-level access..
- **Experience**: Security engineers report higher confidence and lower friction when identifying, reviewing, and fixing risky roles.