Development action items to discuss with the team

Data and APIs

- Agree on what data is needed for each screen: users/roles, permissions, usage history, risk scores, and recommendations.
- Design and build APIs to:
    - Load KPI numbers and the list of entities with filters.
    - Fetch detailed permissions and usage for a selected role.
    - Return recommended fixes and accept a request to apply those fixes.

Risk and recommendation logic

- Define the risk-scoring logic (what makes a permission High, Medium, or Low risk).
- Implement rules to detect unused permissions and overly broad permissions (for example, wildcards or full-access actions).
- Build logic that converts these findings into clear actions: “Remove,” “Restrict,” or “Review.”

Frontend and flow

- Create reusable components for KPI cards, filters, tables, risk badges, and the three-column comparison view.
- Implement the end-to-end flow:
    - Screen 1: overview and triage
    - Screen 2: role details and recommended fixes
    - Screen 3: confirmation and “Apply Fix”
- Make sure filters and selections are preserved when moving between screens.

Security, auditing and safety nets

- Ensure only authorized users can see and change IAM data in this tool.
- Log all important actions (viewing a role, applying fixes, rolling back) for audit purposes.
- Consider a “dry-run” or preview mode and, where possible, a way to restore the previous policy if something goes wrong.

Testing and success tracking

- Add tests for risk scoring, detection rules, and the full remediation flow, including error cases.
- Track key metrics such as time to remediate a high-risk role, number of fixes applied, and any rollbacks caused by changes.
- Use these metrics to refine the recommendations and improve the product over time.