Deepfake Case Management CRM – Incident Reporting & Investigation System

🔲 Problem Statement

Social media platforms, governments, and organizations face increasing challenges due to **deepfake content**.

- Victims find it hard to **report incidents**.
- Investigations are **slow and uncoordinated**.
- Evidence tracking and approvals are **manual**.
- No centralized dashboards exist to monitor case progress or trends.

Solution: Implement Salesforce CRM to create a system for reporting, tracking, and resolving deepfake incidents through automation, integrations, and dashboards.

🔲 Use Cases

1. **Incident Reporting**
    - Users report suspected deepfake content through a portal/web form.
    - Case auto-created in Salesforce.
2. **Case Assignment & Investigation**
    - System auto-assigns cases to analysts based on workload/region.
    - Track case status: *New* → *Under Review* → *Escalated* → *Resolved*.
3. **Evidence Management**
    - Store uploaded videos/images as evidence records.
    - Ensure secure access with role-based permissions.
4. **Integration with AI Deepfake Detection Tools**
    - API integration with external ML models to auto-detect authenticity.
    - Store detection results inside Salesforce case.
5. **Reporting & Dashboards**
    - Number of reported cases per month
    - Average resolution time
    - Escalated vs resolved cases
    - Analyst performance

Salesforce Project Phases Mapping

Phase 1: Problem Understanding & Industry Analysis

- Study the rise of deepfake issues in media & security industries.
- Stakeholder interviews: victims, moderators, analysts, compliance officers.
- Benchmark: Google DeepMind, Microsoft Video Authenticator tools.

Phase 2: Org Setup & Configuration

- Salesforce Enterprise Edition setup.
- Users: Case Reporters, Analysts, Managers, Compliance Team.
- Roles: Reporter → Analyst → Manager → Compliance Officer.
- Profiles with restricted permissions (evidence access).

Phase 3: Data Modeling & Relationships

- Custom Objects:
  - **Deepfake Case** (incident details)
  - **Evidence** (videos, screenshots)
  - **Investigation Report** (analyst notes)
- Relationships:
  - Case ↔ Evidence (One-to-Many)
  - Case ↔ Investigation Report (One-to-One)

Phase 4: Process Automation (Admin)

- Validation Rule: Case cannot close without at least one evidence file.
- Flow: Auto-assign cases based on region/workload.
- Approval Process: Final case closure requires Manager approval.
- Email Alerts: Notify reporter when case status changes.

Phase 5: Apex Programming (Developer)

- Trigger: Update “Investigation Status” when AI detection result is received.
- Queueable Apex: Bulk verification of cases through AI API.
- Future Method: Send asynchronous callouts to external detection API.
- Exception Handling: API failures logged automatically.

Phase 6: User Interface Development

- Lightning App: *Deepfake Case Management*.
- Record Page: Case details + embedded AI authenticity score.

- LWC Component: File preview (evidence) + “Run Deepfake Check” button.

Phase 7: Integration & External Access

- REST API integration with external AI detection service.
- Salesforce Connect for linking external databases (law enforcement data).
- OAuth for secure API calls.

Phase 8: Data Management & Deployment

- Data Import Wizard: Upload initial sample cases.
- Change Sets for deployment to production.
- VS Code + SFDX for version control.

Phase 9: Reporting, Dashboards & Security Review

- Dashboards:
  - Reported vs Resolved Deepfake Cases
  - Average Investigation Time
  - Analyst Productivity
- Security Review:
  - Field-level security for sensitive evidence
  - Audit Trail for approvals

Phase 10: Final Presentation & Demo Day

- Live Demo: User reports deepfake → case auto-assigned → AI check → manager approves resolution.
- Pitch Deck: Showcase how CRM improves trust, reduces investigation time.
- Feedback collection from stakeholders.
- Documentation + Portfolio/LinkedIn showcase.