Sensitive Data Analysis for TechCorp Inc.

Objective

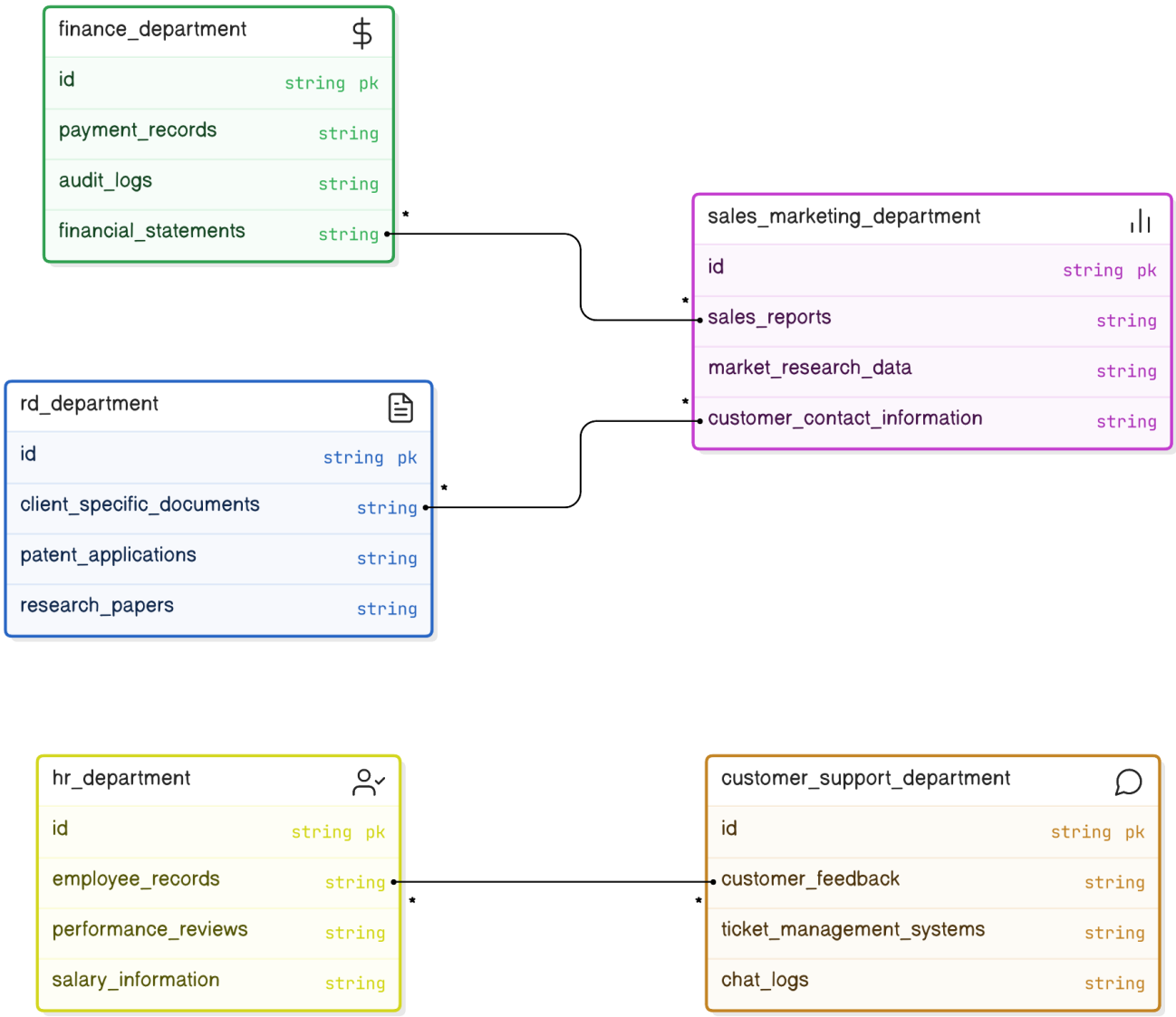
Conduct a sensitive data analysis for TechCorp Inc., a mid-sized software development company specializing in custom software solutions across various industries. The task involves identifying and classifying types of sensitive data, mapping out data flows, and assessing potential risk points within the organization.

Project Tasks

1. Identify and Classify Sensitive Data

a) Identifying Potential Sensitive Data

- **Human Resources (HR) Department:**
  - Employee records (PII, financial data)
  - Performance reviews
  - Salary information
- **Finance Department:**
  - Financial statements (financial data)
  - Payment records
  - Audit logs
- **Research and Development (R&D) Department:**
  - Patent applications (intellectual property)
  - Research papers
  - Client-specific development documents
- **Customer Support Department:**
  - Customer feedback (PII, customer data)
  - Ticket management systems
  - Chat logs
- **Sales and Marketing Department:**
  - Sales reports (financial data, customer data)
  - Market research data
  - Customer contact information



Identifying Potential Sensitive Data

b) List of Sensitive Data Types by Department

- **HR Department:**
    1. Employee records
    2. Performance reviews
    3. Salary information
    4. Benefits documentation
    5. Training records
- **Finance Department:**
    1. Financial statements
    2. Payment records
    3. Tax documents
    4. Investment portfolios

5. Audit logs

- **R&D Department:**

1. Patent applications
2. Research papers
3. Development plans
4. Client-specific development documents
5. Prototypes and designs

- **Customer Support Department:**

1. Customer feedback
2. Ticket management systems
3. Chat logs
4. Help desk records
5. Knowledge base content

- **Sales and Marketing Department:**

1. Sales reports
2. Market research data
3. Customer contact information
4. Lead generation tools
5. Advertising campaigns

c) Classify Each Type of Data

Sensitive Data Type	Classification
Employee records	High
Performance reviews	Medium
Salary information	High
Benefits documentation	High
Training records	Medium
Financial statements	High
Payment records	High
Tax documents	High
Investment portfolios	High
Audit logs	High
Patent applications	High
Research papers	High
Development plans	High

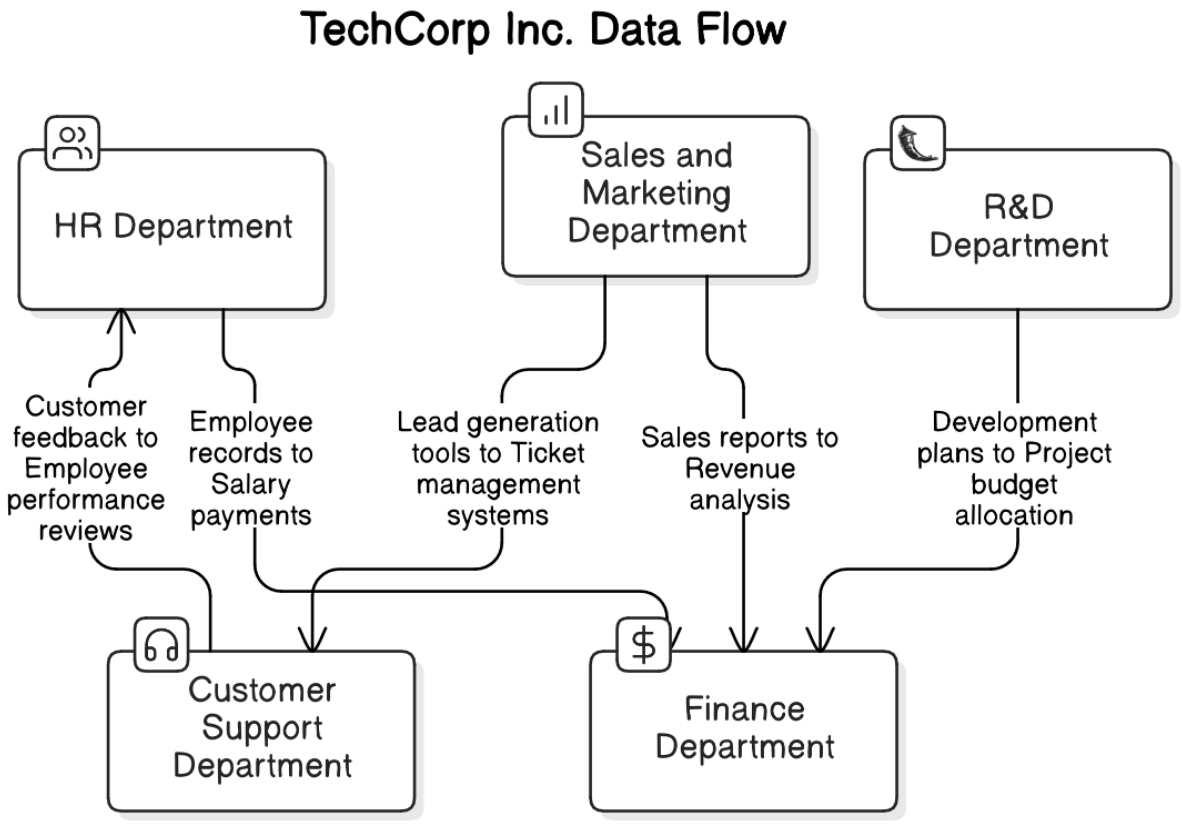
Sensitive Data Type	Classification
Client-specific development documents	High
Prototypes and designs	Medium
Customer feedback	Medium
Ticket management systems	Low
Chat logs	Medium
Help desk records	Low
Knowledge base content	Low
Sales reports	Medium
Market research data	Medium
Customer contact information	High

2. Map Data Flows and Risk Points

a) Mapping Data Flows

1. HR Department → Finance Department:
    - Employee records → Salary payments
2. R&D Department → Finance Department:
    - Development plans → Project budget allocation
3. Sales and Marketing Department → Customer Support Department:
    - Lead generation tools → Ticket management systems
4. Customer Support Department → HR Department:
    - Customer feedback → Employee performance reviews
5. Sales and Marketing Department → Financial Department:
    - Sales reports → Revenue analysis

Data Flow Diagram:



b) Identified Risk Points

1. **Risk Point 1:**
    - **Scenario:** An employee in the Finance Department accesses sensitive data related to a recent financial audit.
    - **Control Suggestion:** Implement multi-factor authentication (MFA) for access to finance-related data.
2. **Risk Point 2:**
    - **Scenario:** A customer support representative shares PII on a public chat platform.
    - **Control Suggestion:** Enforce strict guidelines for communication channels and regularly review logs for compliance.
3. **Risk Point 3:**
    - **Scenario:** R&D engineers discuss project details in an unsecured cloud storage environment.
    - **Control Suggestion:** Encrypt all data stored in the cloud, especially intellectual property documents.

3. Report Your Findings

Analysis Report

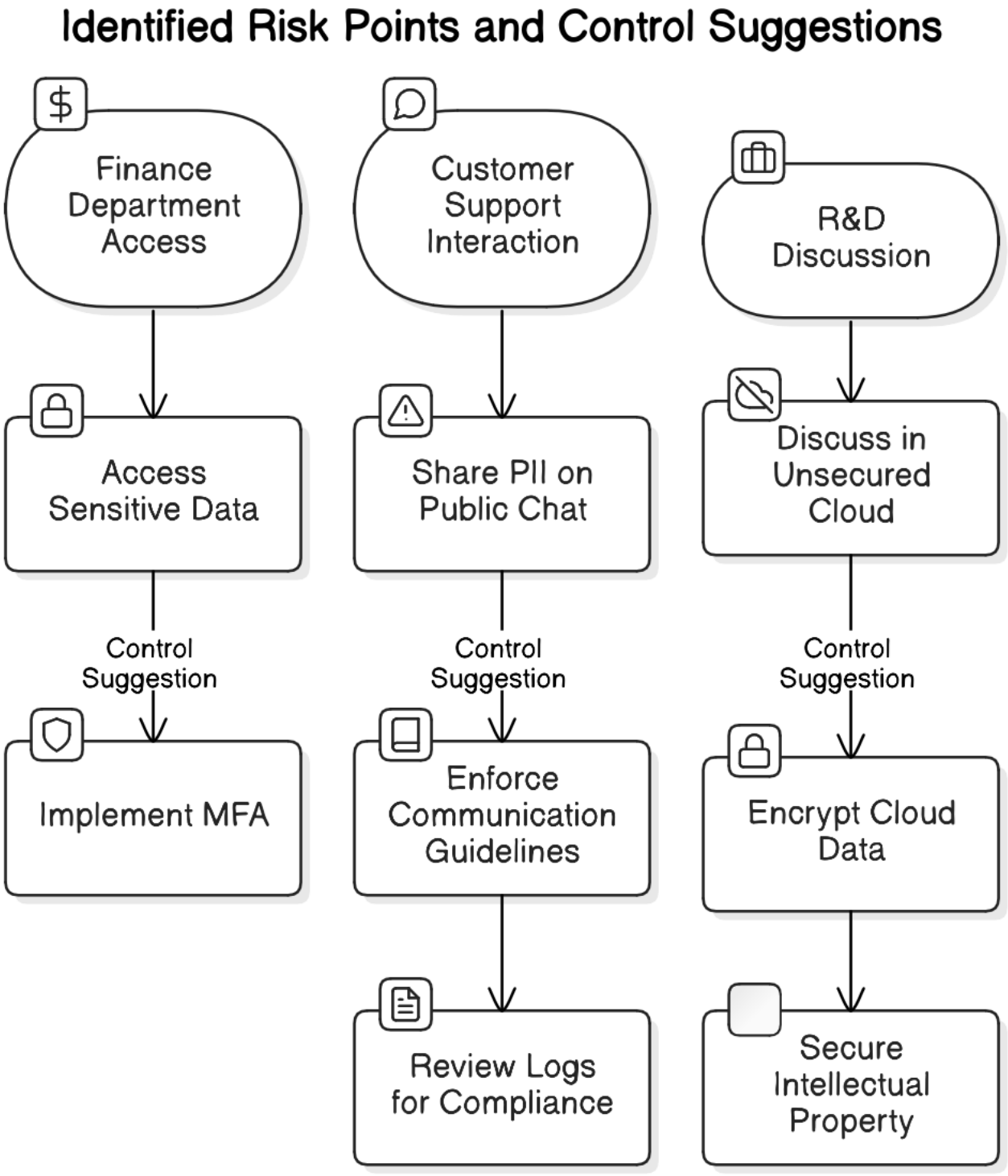
Sensitive Data Inventory:

Department	Sensitive Data Types
HR	Employee records, performance reviews, salary information, benefits documentation, training records
Finance	Financial statements, payment records, tax documents, investment portfolios, audit logs
R&D	Patent applications, research papers, development plans, client-specific development documents, prototypes and designs
Customer Support	Customer feedback, ticket management systems, chat logs, help desk records, knowledge base content
Sales and Marketing	Sales reports, market research data, customer contact information, lead generation tools, advertising campaigns

Data Classification:

- High Sensitive Data:
    - Employee records
    - Financial statements
    - Tax documents
    - Patent applications
- Medium Sensitive Data:
    - Performance reviews
    - Payment records
    - Sales reports
    - Research papers
    - Chat logs
- Low Sensitive Data:
    - Ticket management systems
    - Help desk records
    - Knowledge base content
    - Lead generation tools
    - Advertising campaigns

Data Flow Diagram:



Risk Points and Controls:

1. **Risk Point:** Access to finance-related data by HR employees.
    - **Control:** Implement MFA for access to finance-related data.
2. **Risk Point:** Sharing PII on public chat platforms by customer support representatives.
    - **Control:** Enforce strict communication guidelines and regularly review logs for compliance.

3. **Risk Point:** Discussion of project details in an unsecured cloud storage environment by R&D engineers.
    - **Control:** Encrypt all data stored in the cloud, especially intellectual property documents.