Business Requirements Document (BRD)

AI-Enhanced Data Privacy and Compliance Monitoring with AI Agents

Prepared By: Rahul Singh

Date: June 08, 2025

1 Project Overview

The AI-Enhanced Data Privacy and Compliance Monitoring project aims to deploy a system leveraging AI agents to autonomously identify, classify, and monitor sensitive data (e.g., Personally Identifiable Information (PII), financial, health data) across an organization's infrastructure. These agents will use natural language processing (NLP), machine learning (ML), and privacy-preserving techniques like zero-knowledge machine learning (zkML) to ensure compliance with regulations such as GDPR, CCPA, and HIPAA, while detecting and mitigating unauthorized access or data exfiltration attempts. The use of AI agents enhances automation, scalability, and adaptability to address increasing cyber threats and regulatory scrutiny.

2 Business Objectives

- **Enhance Regulatory Compliance**: Automate data classification and compliance monitoring using AI agents to ensure adherence to GDPR, CCPA, HIPAA, and other regulations.
- **Reduce Data Breach Risks**: Deploy real-time monitoring agents to detect and respond to unauthorized access or data exfiltration, minimizing financial and reputational damage.
- **Improve Operational Efficiency**: Utilize reporting agents to automate compliance reporting and audit processes, reducing manual effort by 50%.
- **Enhance Data Privacy**: Implement privacy-preserving agents to balance security monitoring with user privacy, maintaining trust and ethical standards.
- **Scalability and Adaptability**: Build a distributed agent-based system that integrates with diverse environments (on-premises, cloud, hybrid) and adapts to evolving regulations and threats.

3 Scope

3.1 In-Scope

- Deployment of AI agents for:
  - Automated identification and classification of sensitive data in structured (databases) and unstructured (emails, documents) formats.
  - Real-time anomaly detection for unauthorized data access or exfiltration.
  - Automated compliance reporting for regulatory audits (e.g., GDPR Article 30, CCPA).
  - Integration with existing security systems (e.g., SIEM, IAM).
  - Privacy-preserving analysis using zkML or federated learning.

- Support for cloud (AWS, Azure, GCP), on-premises, and hybrid environments.
- Web-based dashboard for agent management and monitoring.

3.2 Out-of-Scope

- Physical security monitoring (e.g., CCTV integration).
- Development of new regulatory frameworks or policies.
- Implementation of non-AI-based monitoring tools.
- Support for non-standard data formats not specified in requirements.

4 Stakeholders

- **Executive Sponsor**: Chief Information Security Officer (CISO).
- **Project Manager**: IT Project Lead.
- **End Users**: Data protection officers, compliance teams, IT security teams.
- **External Stakeholders**: Regulatory bodies (e.g., GDPR supervisory authorities), auditors.
- **Vendors/Partners**: AI platform providers (e.g., IBM Guardium), cloud service providers.

5 Business Requirements

5.1 BR1: Data Identification and Classification

- AI agents must autonomously identify and classify sensitive data (e.g., PII, financial, health records) across structured and unstructured sources.
- Classification accuracy must exceed 95% for common data types (e.g., names, addresses, credit card numbers).
- Agents must support customizable classification policies via a web interface.

5.2 BR2: Real-Time Monitoring and Anomaly Detection

- Monitoring agents must track data access and usage in real-time, detecting anomalies (e.g., unusual data transfers, unauthorized access).
- Anomaly detection must achieve a false positive rate of less than 5%.
- Agents must prioritize and deliver alerts based on severity via email, SIEM, or SMS.

5.3 BR3: Compliance Reporting

- Reporting agents must generate automated reports for regulatory audits, including data inventory, access logs, and incident summaries.

- Reports must comply with GDPR Article 30, CCPA, and HIPAA requirements.
- Reports must be exportable in PDF and CSV formats and stored for 3 years.

5.4 BR4: Integration with Existing Systems

- Integration agents must connect with SIEM (e.g., Splunk, QRadar) and IAM systems (e.g., Okta, Azure AD) via APIs.
- Support cloud platforms (AWS, Azure, GCP) with latency under 500 milliseconds.

5.5 BR5: Privacy-Preserving Techniques

- Privacy-preserving agents must use zkML or federated learning to protect sensitive data during analysis.
- Agents must ensure no unauthorized PII exposure and provide audit logs for transparency.

5.6 BR6: Scalability and Performance

- Agents must scale to handle 1 petabyte of data across distributed environments.
- Response time for anomaly detection must be under 1 second for critical alerts.

5.7 BR7: User Interface

- A web-based dashboard must allow management of AI agents, displaying real-time alerts, data inventories, and compliance status.
- Support role-based access control (RBAC) and multi-language options.

6 Assumptions

- Data repositories (databases, file servers, cloud storage) provide API access or log exports.
- Regulatory requirements (e.g., GDPR, CCPA) remain stable during the project timeline.
- IT staff have basic familiarity with AI agent management and maintenance.

7 Constraints

- **Budget**: $500,000 for initial implementation, including software, hardware, and agent deployment.
- **Timeline**: 12 months for full deployment, with a pilot phase within 6 months.
- **Data Privacy**: Must comply with GDPR, CCPA, HIPAA, and ISO 27001.

- **Infrastructure**: Must support hybrid environments without major legacy system overhauls.

8 Risks

- **Data Quality**: Poor-quality data may reduce agent accuracy.
  - *Mitigation*: Use synthetic data and data cleansing pipelines.
- **Regulatory Changes**: Evolving regulations may require agent updates.
  - *Mitigation*: Design agents with modular updates for compliance.
- **Adversarial Attacks**: Attackers may target AI agents via data poisoning.
  - *Mitigation*: Implement robust model validation and monitoring.
- **Privacy Concerns**: Over-monitoring may raise privacy issues.
  - *Mitigation*: Use privacy-preserving agents (zkML, federated learning).

9 Success Criteria

- Achieve 95% accuracy in data classification and anomaly detection.
- Reduce compliance reporting time by 50% compared to manual processes.
- Pass a regulatory audit within 12 months.
- Detect and respond to 90% of unauthorized access attempts in real-time.

10 Approval