# TOGAF Enterprise Architecture for Banking/Healthcare

This document presents the design and implementation of enterprise architecture using TOGAF for the Banking and Healthcare domains. The architecture follows the four primary layers of TOGAF: Business Architecture, Application Architecture, Data Architecture, and Technology Architecture. A vertical Security & Compliance pillar ensures trust and governance across all layers.
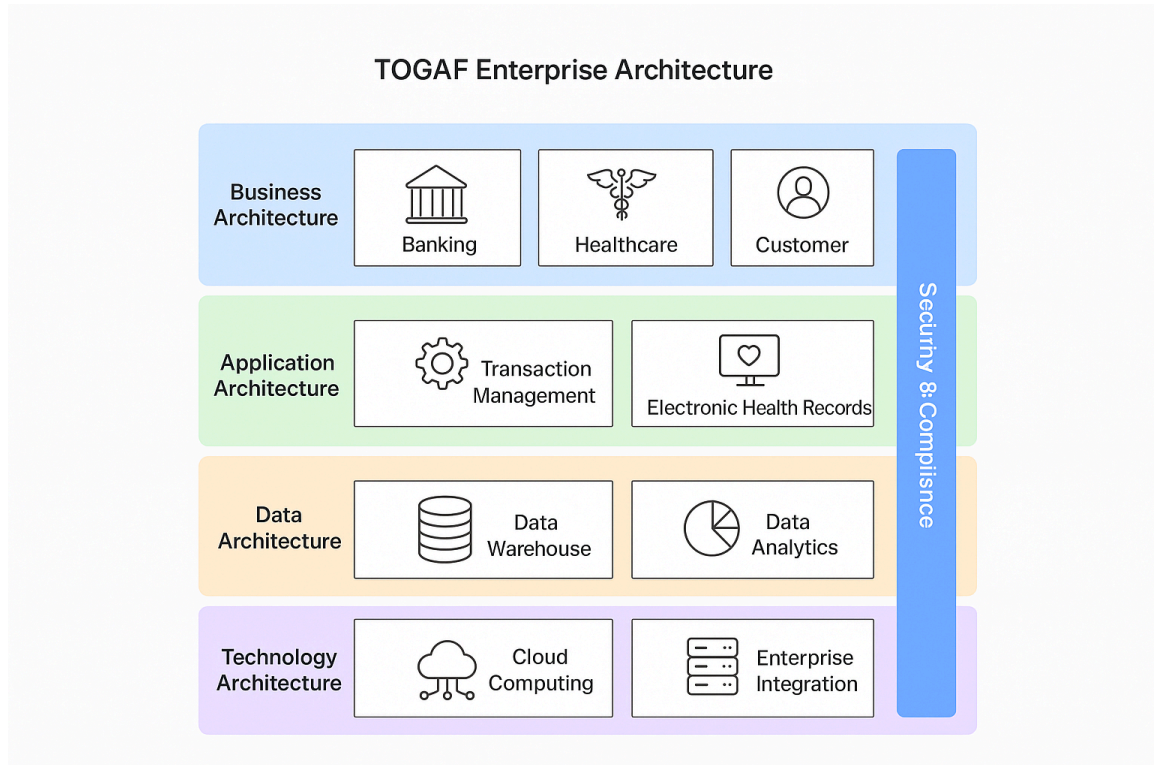
Detailed Layer Explanations

1. Business Architecture

• Banking → Represents financial institutions offering services like savings, loans, and digital banking.
• Healthcare → Represents hospitals, clinics, and medical organizations managing health services.
• Customer → Central to both domains, ensuring customer-centric services and satisfaction.
👉 Defines business goals, processes, and stakeholders.

2. Application Architecture

• Transaction Management (Banking) → Manages secure and efficient processing of financial transactions.
• Electronic Health Records (Healthcare) → Digital systems for storing and accessing patient

data.
👉 Supports business functions with domain-specific applications.

3. Data Architecture

• Data Warehouse → Consolidated storage of banking or healthcare data for analytics.
• Data Analytics → Enables insights into financial trends or patient care outcomes.
👉 Ensures data integrity, accessibility, and effective usage.

4. Technology Architecture

• Cloud Computing → Provides scalable infrastructure to host applications and data securely.
• Enterprise Integration → Ensures smooth interoperability between legacy and modern systems.
👉 Supplies the technical foundation to run business and application services.

5. Security & Compliance (Vertical Layer)

• Runs across all layers ensuring data privacy, security, and adherence to regulations (e.g., GDPR, HIPAA, PCI-DSS).
👉 Protects sensitive financial and health data while ensuring trust and compliance.

Summary

The TOGAF Enterprise Architecture model provides a structured framework for both banking and healthcare. It ensures alignment between business processes, applications, data management, and technology infrastructure. The Security & Compliance pillar enforces regulatory standards and builds customer trust in both critical domains.