

AI-Driven Enterprise Architecture Change Impact Analysis Framework

A Comprehensive Framework for Using AI to Assess Architectural Change, Dependency Impact, Risk, Cost, Compliance, and Transformation Readiness

Sanjeeve Kumar Gajadi*

*(HCL Technologies, Bengaluru, Karnataka, India)

Email: sanjeevekumar.g@hcltech.com

Abstract:

Enterprise architecture change decisions frequently affect applications, data, integrations, business capabilities, infrastructure, security, compliance, and operating models across multiple domains. Traditional impact analysis is often manual, slow, and incomplete because dependency knowledge is distributed across repositories, documents, CMDBs, roadmaps, and subject-matter experts. This paper proposes an AI-Driven Enterprise Architecture Change Impact Analysis Framework that combines architecture knowledge graphs, metadata, dependency models, semantic search, machine learning, Generative AI, and policy rules to evaluate the likely effects of proposed change. The framework defines impact domains, confidence scoring, risk propagation, scenario comparison, evidence traceability, human validation, and governance controls. It supports application modernization, cloud migration, data-platform transformation, API changes, vendor replacement, and AI adoption. The proposed approach enables architects to identify hidden dependencies earlier, reduce design rework, improve decision quality, and create more defensible transformation roadmaps.

Keywords — Enterprise Architecture, Change Impact Analysis, Generative AI, Knowledge Graph, Architecture Governance, Dependency Analysis, Digital Transformation, Risk Analysis, AI-Assisted Architecture, TOGAF

I. INTRODUCTION

Enterprise architecture change rarely occurs in isolation. A single platform, interface, or data-model change can affect many downstream systems and business capabilities.

AI can improve impact analysis by correlating structured architecture metadata with unstructured documents, operational evidence, and dependency relationships.

II. FRAMEWORK OBJECTIVES

The framework aims to identify affected architecture elements, estimate impact severity, explain dependency paths, prioritize validation, and support alternative-scenario comparison.

AI recommendations remain advisory and should be validated by accountable architects and domain owners.

III. ARCHITECTURE KNOWLEDGE FOUNDATION

Reliable impact analysis requires a connected model of capabilities, applications, data, APIs, technology, vendors, risks, controls, roadmaps, and owners.

A knowledge graph can represent these relationships and allow impact propagation across multiple architectural layers.

IV. CHANGE CLASSIFICATION

Changes can be classified by domain, scope, urgency, reversibility, regulatory relevance, and dependency depth.

Classification determines which models, rules, repositories, and human reviewers participate in the analysis.

V. DEPENDENCY DISCOVERY

AI-assisted discovery can extract relationships from solution documents, interface catalogs, code metadata, service registries, data lineage, and operational telemetry.

Discovered dependencies should include confidence scores and evidence references so architects can distinguish verified facts from inferred relationships.

VI. IMPACT SCORING

Impact scoring can combine business criticality, number of dependencies, technical complexity, data sensitivity, security exposure, cost, delivery risk, and change reversibility.

Scores should be calibrated against historical change outcomes and should not hide critical single-point dependencies.

VII. RISK PROPAGATION

Risk propagation evaluates how a local change could create secondary effects such as degraded service, data inconsistency, control failure, or vendor concentration.

Graph-based analysis can highlight high-centrality components whose failure or modification affects multiple business capabilities.

VIII. SCENARIO ANALYSIS

Architects can compare modernization, replacement, coexistence, or phased-transition scenarios using cost, risk, timeline, complexity, and strategic alignment.

Generative AI can summarize tradeoffs while preserving traceability to underlying evidence and assumptions.

IX. GOVERNANCE AND HUMAN VALIDATION

High-impact recommendations should require validation by business, security, data, infrastructure, and application owners where appropriate.

Approval records should capture assumptions, accepted risks, rejected alternatives, and the rationale for the selected architecture decision.

X. IMPLEMENTATION ROADMAP

Organizations can begin with high-quality architecture inventories and a small set of trusted dependency sources before expanding AI-assisted inference.

Maturity can progress toward continuous impact analysis triggered by repository, code, data, and cloud configuration changes.

XI. METRICS AND BENEFITS

Useful metrics include analysis lead time, hidden dependencies discovered, design rework avoided, decision cycle time, change failure rate, and stakeholder confidence.

The primary benefit is earlier visibility of cross-domain consequences before implementation cost and operational risk increase.

XII. CONCLUSION

AI-driven change impact analysis can make enterprise architecture more predictive and evidence-based.

By combining connected architecture knowledge, AI inference, scoring, and human governance, enterprises can improve transformation decisions and reduce unintended change consequences.

ACKNOWLEDGMENT

The author acknowledges the contributions of enterprise architecture practitioners, AI governance specialists, standards bodies, security professionals, data leaders, and technology researchers whose published work informed the concepts synthesized in this paper.

REFERENCES

- [1] National Institute of Standards and Technology, Artificial Intelligence Risk Management Framework (AI RMF 1.0), 2023.
- [2] National Institute of Standards and Technology, AI RMF Generative Artificial Intelligence Profile, 2024.
- [3] ISO/IEC 42001:2023, Information technology — Artificial intelligence — Management system.
- [4] ISO 31000:2018, Risk management — Guidelines.
- [5] ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection — Information security management systems.
- [6] The Open Group, TOGAF Standard, 10th Edition, 2022.
- [7] ISACA, COBIT 2019 Framework: Governance and Management Objectives, 2019.
- [8] OWASP Foundation, OWASP Top 10 for Large Language Model Applications.

- [9] MITRE, ATLAS: Adversarial Threat Landscape for Artificial-Intelligence Systems.
- [10] OECD, Recommendation of the Council on Artificial Intelligence.
- [11] SAP SE, SAP Business Technology Platform Documentation.
- [12] SAP SE, SAP Business Data Cloud and SAP Datasphere Documentation.