A Unified Model for Modern Security Architecture

Integrating TOGAF®, SABSA®, COBIT®, and The Open Group Axioms

A White Paper for 2026

Author

Christian Kobsa
Strategic Enterprise Architect & Business Architect
Digital Enterprise Architecture & Advisory (DEAA)

Abstract

Security architecture has evolved into a strategic enterprise capability essential for organizations navigating cloud transformation, distributed identity, AI-driven systems, and increasingly sophisticated adversaries. This white paper presents a unified model that integrates TOGAF®, SABSA®, COBIT®, and The Open Group Axioms into a cohesive, future-proof approach for designing, governing, and operating security architecture in modern enterprises.

Executive Summary

Modern enterprises operate in an environment defined by rapid digital transformation, distributed architectures, cloud adoption, API ecosystems, and increasingly sophisticated adversaries. Security can no longer be treated as a technical afterthought or a collection of isolated controls. It must function as a strategic, business-aligned capability embedded across the entire enterprise architecture landscape.

This white paper introduces a unified model for security architecture that integrates four authoritative frameworks:

- TOGAF® — providing the enterprise architecture structure and lifecycle
- SABSA® — delivering a business-driven, risk-aligned security architecture method
- COBIT® — establishing governance, accountability, and performance measurement
- The Open Group Axioms — offering timeless principles that guide architectural thinking

Together, these components form a cohesive, future-proof approach to designing, governing, and operating security architecture in 2026 and beyond.

The unified model ensures that security architecture is:

- Business-driven, grounded in organizational goals and risk appetite
- Methodologically rigorous, with traceability from business attributes to controls
- Governed and measurable, with clear decision rights and maturity models

Principle-based, leveraging the Axioms to ensure clarity, simplicity, and resilience

Adaptable, supporting modern patterns such as zero trust, cloud-native security, identity fabric, and AI governance

This paper provides a structured narrative, a layered architecture model, and supporting appendices to help organizations adopt this unified approach. The result is a security architecture practice that is consistent, scalable, and aligned with enterprise strategy — enabling organizations not only to protect value, but to create it.

Table of Contents

1. Introduction

Security architecture has historically been fragmented across methods, frameworks, and organizational silos. Enterprise architects often rely on TOGAF without a dedicated security method. Security teams deploy controls without architectural alignment. Governance teams use COBIT without traceability to architectural decisions. The result is predictable: inconsistent controls, duplicated effort, and misalignment with business objectives.

This white paper introduces a unified model that resolves these issues by integrating TOGAF, SABSA, COBIT, and The Open Group Axioms into a single, cohesive practice. The model is designed for organizations seeking a business-driven, risk-aligned, and principle-based approach to security architecture.

2. The Case for a Unified Security Architecture Model

Modern enterprises face challenges that cannot be addressed by technical controls alone:

- Cloud-native platforms and distributed workloads
- Zero trust requirements and identity-centric security
- API ecosystems and microservices
- AI/ML systems requiring governance and assurance
- Regulatory pressure and continuous compliance
- Supply chain and third-party risk

Security architecture must therefore evolve into a **strategic enterprise discipline**, grounded in business value, risk management, and architectural rigor.

A unified model provides:

- **Consistency** across architecture, design, and governance

- **Traceability** from business drivers to controls
- **Clarity** in roles, responsibilities, and decision rights
- **Resilience** through layered, principle-based design
- **Adaptability** to emerging technologies and threats

3. Framework Foundations

3.1 TOGAF®: Enterprise Architecture Backbone

TOGAF provides the structural foundation for integrating security across the enterprise:

- Architecture Development Method (ADM)
- Business, Data, Application, and Technology domains
- Architecture views and viewpoints
- Requirements management
- Governance and compliance structures

In the unified model, TOGAF defines **where** security architecture fits and **how** it integrates across the enterprise lifecycle.

3.2 SABSA®: Security Architecture Method

SABSA provides the methodological rigor required for security architecture:

- Business Attribute Profiles
- Contextual → Conceptual → Logical → Physical → Component layers
- Risk-driven design
- Traceability from business drivers to controls

In the unified model, SABSA defines **how** security architecture is created and **why** each control exists.

3.3 COBIT®: Governance and Oversight

COBIT provides the governance system that ensures security architecture is:

- Accountable
- Measurable
- Compliant
- Effective

COBIT contributes:

- Governance and management objectives
- Control objectives
- Maturity and capability models
- Decision rights and accountability structures

In the unified model, COBIT defines **how security architecture is governed and measured**.

3.4 The Open Group Axioms: Principles for Practice

The Axioms for the Practice of Security Architecture provide timeless guidance, including:

- **Business Risk-Driven Security**
- **Context Awareness**
- **Holistic Approach**
- **Simplicity**
- **Reuse**
- **Resilience**
- **Security by Design**
- **Defense in Depth**

- **Least Privilege and Access Management**

These axioms form the **architectural philosophy** underpinning the unified model.

4. The Unified Model

The unified model integrates the four frameworks into a layered architecture stack.

4.1 Layer 1 — Business Drivers

(TOGAF + SABSA + Axioms)

- Business goals and outcomes
- Risk appetite and tolerance
- Business Attribute Profiles
- Axiom 1: Business Risk-Driven Security
- Axiom 2: Context

This layer ensures that security architecture is aligned with business value.

4.2 Layer 2 — Architecture Method

(SABSA + TOGAF)

- Contextual architecture
- Conceptual architecture
- Logical architecture
- Physical architecture
- Component architecture
- Integration with TOGAF ADM phases

This layer provides the structured method for designing security architecture.

4.3 Layer 3 — Governance and Assurance

(COBIT + Axioms)

- Governance objectives
- Control objectives
- Maturity models
- Performance measurement
- Axiom 10: Process-Driven
- Axiom 11: Optimal Conflict Resolution

This layer ensures accountability, compliance, and continuous improvement.

4.4 Layer 4 — Design Principles

(Axioms)

- Simplicity
- Reuse
- Resilience
- Defense in depth
- Least privilege
- Security by design

These principles guide architectural decisions and ensure long-term sustainability.

4.5 Layer 5 — Implementation and Operations

- Zero trust architectures
- Cloud-native security controls
- Identity fabric and distributed identity
- API and microservices security
- AI/ML governance and assurance
- Continuous compliance and automation

This layer operationalizes the architecture in modern environments.

5. Applying the Unified Model

The unified model supports a wide range of enterprise initiatives:

Cloud Transformation

Ensures secure migration, landing zones, and governance.

Zero Trust Programs

Provides identity-centric, context-aware, risk-aligned architecture.

API Ecosystems

Aligns API security with business attributes and governance.

AI/ML Governance

Integrates model risk, assurance, and ethical considerations.

Regulatory Compliance

Provides traceability from business drivers to controls and evidence.

Enterprise Modernization

Ensures security is embedded across all architecture domains.

6. Benefits of the Unified Model

- **Business alignment** through risk-driven design
- **Architectural consistency** across domains and lifecycle phases
- **Governance clarity** through COBIT integration
- **Principle-based design** guided by the Axioms
- **Future-proofing** through adaptability to emerging technologies
- **Traceability** from business goals to technical controls

7. Conclusion

Security architecture is no longer a technical afterthought. It is a strategic enterprise capability that requires:

- A structured method (SABSA)
- An enterprise integration framework (TOGAF)
- A governance system (COBIT)
- A set of timeless principles (Axioms)

The unified model presented in this white paper provides a coherent, modern, and future-proof approach to security architecture in 2026 and beyond.