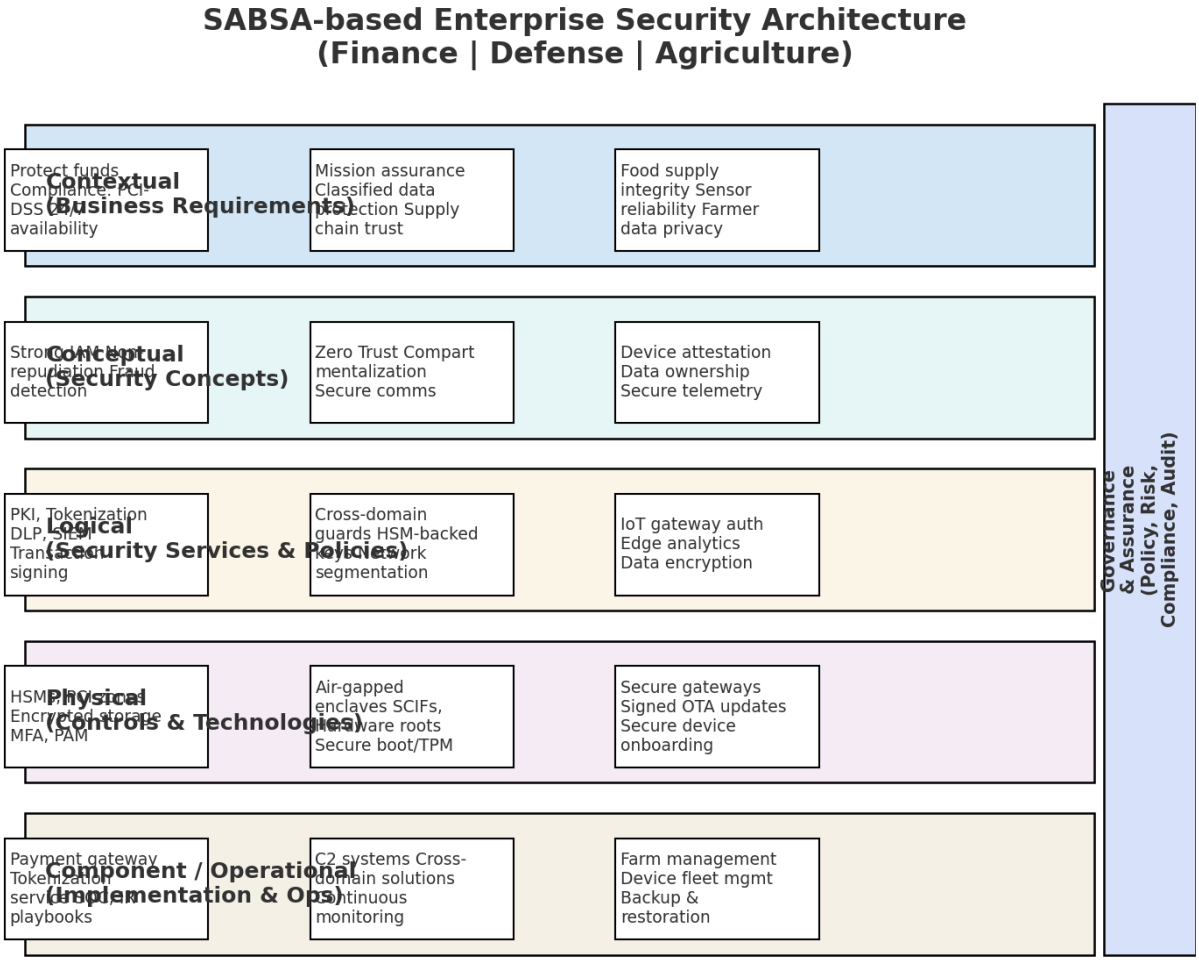
SABSA-based Enterprise Security Architecture

Finance | Defense | Agriculture

This document presents a SABSA (Sherwood Applied Business Security Architecture) based design for enterprise security across three domains: Finance, Defense, and Agriculture. The SABSA approach aligns security architecture with business requirements and drives design through layered abstractions: Contextual, Conceptual, Logical, Physical, and Component/Operational.



SABSA Layers — Explanations and Domain Examples

1. Contextual Layer (Business Requirements)

Purpose: Capture business goals, drivers, stakeholders and the high-level security requirements that justify investments.

Finance Examples:
- Protect customer funds and maintain trust.
- Regulatory compliance (PCI-DSS, GDPR, Anti-Money Laundering).
- High availability for 24/7 banking services.

Defense Examples:
- Mission assurance and continuity of operations.
- Protect classified and controlled unclassified information.
- Supply-chain assurance and trusted suppliers.

Agriculture Examples:
- Ensure integrity of food supply chain and traceability.
- Protect farm/producer data and privacy.
- Reliability of IoT sensors for precision farming.

2. Conceptual Layer (Security Concepts & Models)

Purpose: Define high-level security concepts and services (what is required to meet the contextual requirements).

Common Concepts: Identity & Access Management, Confidentiality, Integrity, Availability, Auditability, Non-repudiation, and Secure Supply Chain.

Finance Example Concepts:
- Strong multi-factor IAM, transaction non-repudiation, fraud analytics.

Defense Example Concepts:
- Zero Trust architecture, data compartmentalization, tactical network isolation.

Agriculture Example Concepts:
- Device attestation, data ownership and consent models, secure telemetry for sensors.

3. Logical Layer (Security Services & Policies)

Purpose: Map concepts into logical security services, policies, and interfaces (how services interact).

Examples of Logical Services:
- PKI and key management, tokenization services, DLP, SIEM/UEBA, secure device provisioning, API gateways, and access policies.

Finance Logical Mapping:
- Transaction signing, tokenization, HSM-backed key lifecycle, real-time fraud detection.

Defense Logical Mapping:
- Cross-domain guards, strong PKI, secure comms, mandatory access controls, enclave-based architectures.

Agriculture Logical Mapping:
- IoT gateway authentication, edge data integrity checks, secure OTA update services.

4. Physical Layer (Controls & Technologies)

Purpose: Specify concrete controls, technology choices, deployment topologies, and operational patterns.

Common Controls: Firewalls, WAF, IDS/IPS, HSMs, TPM/secure boot, encrypted storage, network segmentation, MDM, secure OTA, and cloud security controls.

Finance Physical Example:
- Payment zone architecture (PCI DSS compliance), HSMs for PIN/keys, tokenization, SOC with 24/7 monitoring.

Defense Physical Example:
- Air-gapped/isolated networks for classified systems, hardware roots of trust, SCIFs, specialized cryptographic modules.

Agriculture Physical Example:
- Secure IoT gateways, signed firmware, network segmentation between operational OT and corporate IT, edge compute for resilience.

5. Component / Operational Layer (Implementation & Ops)

Purpose: Build, integrate, operate and maintain the security components — tool selection, vendor integration, runbooks and playbooks.

Examples:
- Finance: Payment gateway components, tokenization service, PAM, SOC, incident response runbooks, audit evidence collection.
- Defense: Command & Control (C2) systems with cross-domain solutions, secure update pipelines, stringent accreditation and continuous monitoring.
- Agriculture: Farm management platforms, device fleet management (onboarding/offboarding), backup/restore for critical telemetry, and service-level monitoring.

Threat Models & Typical Attack Scenarios

Finance:
- Threats: Account takeover, fraudulent transactions, insider fraud, DDoS targeting payment gateways.
- Key Controls: Strong IAM, transaction anomaly detection, tokenization, HSMs, DDoS protection, insider threat monitoring.

Defense:

- Threats: Espionage, supply chain compromise, advanced persistent threats (APTs), insider sabotage.
- Key Controls: Zero Trust, hardware roots of trust, strict supply-chain vetting, multiplicity of monitoring, compartmentalization.

Agriculture:
- Threats: Sensor spoofing/tampering, ransomware on agro-management platforms, false telemetry impacting automated actuators.
- Key Controls: Device attestation, signed OTA, network segmentation, offline operational fallbacks, backup/restore strategies.

Compliance & Regulatory Considerations

Finance: PCI-DSS, SOX, GLBA, local banking regulations, AML/KYC requirements, GDPR for customer personal data.

Defense: NIST frameworks (e.g., SP 800-53), CMMC (for U.S. DoD contractors), ITAR for export-controlled data, national security rules.

Agriculture: GDPR where personal data exists, food-safety traceability requirements, national agricultural data governance rules; generally ISO 27001 can be used as the baseline.

Implementation Roadmap (Phased)

1. Prepare & Assess: Stakeholder workshops, data classification, current-state security assessment, threat modeling.
2. Architect: Define SABSA artifacts across layers — business attributes, trust model, security services, controls.
3. Build & Pilot: Implement core services (IAM, PKI, SIEM, device provisioning) and run pilot in a confined environment.
4. Deploy: Roll-out domain-specific controls (PCI zones, air-gapped segments, secure IoT gateways) with change management.
5. Operate & Improve: SOC/SIEM, continuous monitoring, vulnerability management, exercises, and regular compliance audits.

Metrics, KPIs & Continuous Assurance

Suggested KPIs:
- Mean Time to Detect (MTTD)
- Mean Time to Respond (MTTR)
- Patch compliance percentage
- % of sensitive data encrypted at rest and in transit
- Number of resolved audit findings
- Fraud rate (Finance) / Mission-impacting incidents (Defense) / Data-integrity incidents (Agriculture)

Continuous Assurance:
- Regular control testing, red-team/blue-team exercises, supply-chain audits, and automated compliance checks (CSPM, Cloud Audit tools).

Example: Finance — Secure Payment Processing (Detailed Walkthrough)

Contextual: Business needs guaranteed integrity of transactions, non-repudiation, and compliance with PCI-DSS.

Conceptual: Provide transaction signing, tokenization, and real-time fraud detection as core concepts.

Logical: PKI for certificate management, tokenization service API, SIEM with real-time analytics, strict access policies for payment systems.

Physical: Use HSMs for key storage and PIN processing, segmented PCI-compliant network zones, WAFs on payment endpoints, DDoS mitigation services.

Component/Operational: Deploy payment gateway components, integrate with third-party acquirers, operate a 24/7 SOC, perform PCI audits, and maintain incident response playbooks.